A Report for the World Bank on

Legal and Regulatory Implications of Disruptive Technologies in Emerging Market Economies

June 2018

Professor Ian Walden and Dr Theodora A Christou

Queen Mary University of London
Centre for Commercial Law Studies

Contents

Terms of Reference

This report is prepared for the World Bank Legal Department's Thematic Working Group on Technology and Innovation in Development. The research paper explores the legal issues and considerations the World Bank should take into account when considering financing projects with components that involve disruptive technologies. The report highlights legal and regulatory issues which may either enable or which may impede the adoption or creation of disruptive technologies, particularly in emerging market economies.

The authors of the report are Professor Ian Walden and Dr Theodora A Christou, members of the **Cloud Legal Project** at the Centre for Commercial Law Studies, Queen Mary University London.[1]

[1] http://www.cloudlegal.ccls.qmul.ac.uk

Introduction

Much of the innovation driving the Fourth Industrial Revolution is powered by disruptive technologies. However, as with the discourse of globalisation, they challenge traditional legal frameworks which are often unable to adjust quickly enough to the technological innovations, territorial disconnection, and increased speed and mobility of goods, services, money, people and data. It is important to note from the outset that there does not exist a single model legal framework to govern disruptive technologies. At best what can be hoped for is proper regulation of issues which form part of a broader legal framework incorporating industry or platform led norms and standards. These standards and norms created and promulgated by private actors are a key part of the framework governing disruptive technologies, they facilitate the rapid entry and adoption of new technologies. They need to be aligned with the fundamental principles and mandatory laws of nation states in order to obtain legitimacy and authority. The aim of this paper is to highlight some of the legal and regulatory considerations which should form part of a core legal framework, that can facilitate the adoption of disruptive technologies in emerging market economies and identify those matters which may act as obstacles.

The division between the developed and developing world, despite never having a clear meaning, is also not very useful for the purposes of development. In addition to the use of regional groupings, the starting point increasingly used instead is based on 4 income levels; low, lower-middle, upper-middle and high income groups.[2] With low and medium income taking in those previously referred to as developing countries. Beyond this, any further categorisation of countries into groups will depend on the reasons for requiring the division. The purpose of requiring differentiating markers will depend on the specific objective. For the purposes of this report we highlight particular issues for low and medium income and refer to them with the term 'emerging market economies', since the objective is to further economic development in these countries.

Disruptive technologies cover a plethora of technologies and applications which are either already in use or emerging digital innovations. Disruptive technologies include but are not limited to artificial intelligence; geospatial technology; nano-technology; drones, cloud-based technologies; the Internet of Things; blockchain and distributed ledger technologies, including cryptocurrencies and smart contracts; FinTech; and RegTech. Whilst leaders in innovation generally come from the private sector, this does not take away from the relevance of disruptive technologies for the public sector. In addition to public-private initiatives, governments can deploy technologies to increase its own efficiency, transparency, and accessibility. Government uses of technology to deliver services include land registry, voting, identification, healthcare, company registration, taxation, by port authorities and for supply chain traceability amongst others.[3] It may be that initially the technology is imported, but if local technical capacity is increased then innovation can come from inside the country.

This paper will first take each disruptive technology listed above, define the technology for the purposes of this report and identify some potential applications, before highlighting legal and regulatory considerations specific to them which should be taken into account when it comes to assessing and preparing the legal and regulatory environment. We will then set out the general laws and regulations which are integral to all and have direct applicability to disruptive technologies, namely Data Protection, Cybersecurity, and Intellectual

[2] For further detail on how the World Bank categorises countries, see: https://datahelpdesk.worldbank.org/knowledgebase/articles/378834-how-does-the-world-bank-classify-countries

[3] The potential uses for development and by governments are considered in the GSMA/Deloitte Paper, Blockchain for Development (2017), available at: https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2017/12/Blockchain-for-Development.pdf See also Mark White, Jason Killmeyer, and Bruce Chew, Will blockchain transform the public sector? Blockchain basics for government, September 11, 2017 Deloitte Insights. Available at: https://www2.deloitte.com/insights/us/en/industry/public-sector/understanding-basics-of-blockchain-in-government.html

Property. The final section will summarise the legal and regulatory elements which have the ability to enable and those which have the propensity to inhibit innovation and the adoption of disruptive technologies in emerging market economies.

Disruptive Technologies

We turn now to the individual disruptive technologies, their potential applications, in particular with reference to emerging market economies, and the impact of the legal and regulatory environment on innovation and adoption. Definitions are not always definitive or easy to formulate because the component parts of the underlying technologies are fluid and therefore it can be difficult to distinguish one from the other. So below we set out are the basics relevant for the purposes of this paper. Additionally, the uses we list are by no means exhaustive, they are merely illustrative of the range of issues that will need to be grappled with in an attempt to create a conducive legal environment. The value of disruptive technologies often arise through incremental innovations coupled with unexpected use cases.

Artificial Intelligence

Artificial Intelligence (AI) is defined in the Oxford Dictionary as the "computer systems able to perform tasks normally requiring human intelligence, such as visual perception, speech recognition, decision making and translation between languages." There are three capabilities of AI: (1) Understanding; (2) Reasoning; and (3) Learning. AI is the broader concept of thinking machines which can carry out activities we consider intelligent.

Machine learning is a subset of AI with foundations in statistics and mathematical optimization and the use of algorithms. It can either be supervised or unsupervised learning to predict, analyse or data mine. It has been defined as "the field of computer science dedicated to solving cognitive problems commonly associated with human intelligence, such as learning, problem solving, and pattern recognition."[4] Deep learning takes machine learning to another level through the use of a number of algorithms Deep learning is a new set of methods that is changing machine learning in fundamental ways. Deep learning which implement deep networks with unsupervised learning.

Cognitive computing is another subfield of AI which uses cognitive science knowledge to build systems that simulate the human thought processes.

Robotics use sensors to sense heat and temperature, hear sound, react to pressure and computer vision. The following table goes into further detail on the categories of artificial intelligence. [5]

[4] https://aws.amazon.com/machine-learning/what-is-ai/

[5] Footnotes from table: (3) David Schatsky and Vikram Mahidhar, Intelligent automation: A new era of innovation, Deloitte University Press, January 22, 2014, https://www2.deloitte.com/insights/us/en/focus/signals-for-strategists/intelligent-automation-a-new-era-of-innovation.html (4) BMWA, "What is computer vision" http://www.bmva.org/visionoverview

Categories	Descriptions	Application examples
Robotic process automation (RPA)	"A combination of artificial intelligence and automation" that's able to "sense and synthesize vast amounts of information and can automate entire processes or workflows, learning and adapting as it goes."[3]	• Process automation and configuration • Graphical user interface (GUI) automation • Advanced decision systems
Cognitive—language technologies	A set of statistical techniques that enable the analysis, understanding, and generation of human languages to facilitate interfacing with machines in written and spoken contexts, that is, to convert human (natural) languages into machine languages and vice-versa	• Natural language processing and generation • Semantic computing • Speech recognition • Speech synthesis • Sentiment and text analytics
Cognitive—machine learning (ML)	A set of statistical techniques that automate analytical model-building using algorithms that iteratively learn from data without the need for explicit programming	• Supervised learning • Unsupervised learning • Deep learning
Cognitive—computer vision	Automatic extraction, analysis, and understanding of useful information from a single image or a sequence of images, thereby modeling, replicating, and, more importantly, exceeding human vision using computer software and hardware[4]	• Image recognition • Video analysis • Handwriting recognition • Voice recognition • Optical character recognition

Source: David Schatsky, Craig Muraskin, and Ragu Gurumurthy, *Demystifying artificial intelligence*, Deloitte University Press, November 4, 2014; Tiffany Dovey Fishman, William D. Eggers, and Pankaj Kishnani, *AI-augmented human services*, Deloitte University Press, October 18, 2017; and Deloitte analysis.

AI applications can be used as experts to provide a reasoned explanation and advice to end users, chatbots can communicate with the user in natural language, neural systems can predict the future on the basis of historical data, and it can be used in gaming to engage in strategic moves.

There is an element of AI found in the other disruptive technologies we look at in this paper, such as drones. The existential public concern is that AI will replace humans, however for the most part AI technology is about amplifying human cognitive capability.

It is evident that AI has positive uses especially in the field of development. AI can collect and analyse data at unprecedented rates, but it can also provide humans with answers to questions or confirm hypotheses, thereby speeding up diagnosis by doctors whilst taking into account the latest medical findings in published papers. AI can increase the efficiency of industrial operations. Its monitoring capabilities can identify damage to equipment located in isolated/harsh locations and if necessary carry out repairs. AI also powers commerce, such as Amazon and Netflix to give customers recommendations based on their purchase or viewing history.

One well-known AI service is IBM's Watson which made its debut on the American quiz gameshow Jeopardy! Since then it has been developed and has many active uses, including by the Weather Company which utilises sensors located all over cities to transmit data which is then analysed to provide real-time weather forecasts to billions of users. It is also used by Woodside (an oil and gas company), which has processed tens of thousands of documents relating to the build and operation of oil rigs so that it can check in real time and get answers to questions which would ordinarily require many hours of consultation with experts. Others include

monitoring and identifying cyberbullying for Twitter. The following table[6] lists some industry specific applications, including for the public sector.

Industries	Current applications	Potential applications on the horizon
Financial services	- Automated fraud detection in credit cards, insurance, etc - Automated execution of stock trades[7]	- Improve performance of funds[8] - Detect market manipulation[9]
Health care	- Transcribing/interpreting notes dictated by physicians - Automated medical imaging and mammography[10]	- Automated and more accurate diagnosis[11] - Predicting and analysing treatments[12]
Life sciences	- Drug discovery and development[13]	- Smart supply chains[14]
Public sector	- Answering citizen queries through chatbots[15] Disease surveillance[16]	- Predictive emergency management - Predictive policing[17]
Oil and gas	- Locate energy and mineral deposits[18] - Predictive equipment and assets[19]	- Optimizing energy flow out of batteries and points of consumption[20]

[6] Replicated from Cognitive technologies: A technical primer, February 06, 2018. https://www2.deloitte.com/insights/us/en/focus/cognitive-technologies/technical-primer.html

[7] F McGuire, "JPMorgan to unveil robot to execute stock trades," *Newsmax*, August 1, 2017. https://www.newsmax.com/Finance/StreetTalk/jpmorgan-robots-stock-trades/2017/08/01/id/805123/

[8] Mike Sheen, "Baillie Gifford to leverage AI for fund performance boost," *Investment Week*, August 14, 2017. https://www.investmentweek.co.uk/investment-week/news/3015556/baillie-gifford-to-leverage-ai-in-performance-push

[9] Fortune, "How artificial intelligence could catch stock market cheaters," October 25, 2016. http://fortune.com/2016/10/25/how-artificial-intelligence-could-catch-stock-market-cheaters/

[10] Stacy Lawrence, "GE, Arterys ready launch for deep learning diagnostic system for cardiac MRIs," *Fierce Biotech*, February 18, 2016. http://www.fiercemedicaldevices.com/story/ge-arterys-ready-launch-deep-learning-diagnostic-system-cardiac-mris/2016-02-18;

[11] IBM, "Memorial Sloan-Kettering Cancer Center, IBM to collaborate in applying Watson technology to help oncologists," press release, March 22, 2012. https://www-03.ibm.com/press/us/en/pressrelease/37235.wss

[12] Fei Jiang et.al., "Artificial intelligence in healthcare: Past, present and future," *Stroke and Vascular Neurology*, June 2017. http://svn.bmj.com/content/svnbmj/early/2017/07/29/svn-2017-000101.full.pdf

[13] Monica Heger, "AstraZeneca launches genomics initiative to drive drug discovery and development," *GenomeWeb*, April 21, 2016. https://www.genomeweb.com/sequencing-technology/astrazeneca-launches-genomics-initiative-drive-drug-discovery-and-development

[14] Kim S. Nash, "Merck deploys AI for 'self-driving' supply chain," *Wall Street Journal*, December 20, 2016. https://www.genomeweb.com/sequencing-technology/astrazeneca-launches-genomics-initiative-drive-drug-discovery-and-development

[15] Alka Bahal, "USCIS launches a virtual assistant and her name is EMMA," *Immigration View*, December 16, 2015. https://blogs.wsj.com/cio/2016/12/20/merck-deploys-ai-for-self-driving-supply-chain/; Frost & Sullivan, "2016 global conversational AI and intelligent assistants technology innovation award," 2016. http://www.nextit.com/downloads/Next-IT-Award-Write-Up.pdf

[16] MathWorks, "Centers for Disease Control and Prevention automates poliovirus sequencing and tracking," 2015. https://www.mathworks.com/tagteam/84356_91834v01_CDC_UserStory.pdf

[17] Matt Meuse, "Vancouver police now using machine learning to prevent property crime," *CBC News*, July 22, 2017. http://www.cbc.ca/news/canada/british-columbia/vancouver-predictive-policing-1.4217111

[18] Lindsay Dodgson, "At the speed of thought: Cognitive technology in oil & gas," *Offshore Technology*, May 31, 2016. http://www.offshore-technology.com/features/featureat-the-speed-of-thought-cognitive-technology-in-oil-gas-4872475/

[19] Sundeep Sanghavi, "Why the time is right for cognitive predictive maintenance in oil, gas," *Hart nergy*, October 4, 2017. https://www.epmag.com/blog/why-time-right-cognitive-predictive-maintenance-oil-gas-1661181

[20] Phil Goldstein, "What is the potential for AI in the energy industry?," *BizTech*, October 25, 2017. https://biztechmagazine.com/article/2017/10/what-potential-ai-energy-industry

Industries	Current applications	Potential applications on the horizon
Manufacturing	- Identify product defects, conduct quality checks, detect causes of incidents, and analyse incident trends[21]	- Automated planning of business operations

Drones

Drones are unmanned flying instruments used by the military but increasingly by private individuals for commercial, personal use or development programmes. They come in all sizes from large drones equipped with bombs to ones disguised as mosquitos. AI technology can also operate drones to aid in the identification of crop disease and to remotely treat it; deliver medical supplies to remote areas and mitigate the impact of famines by monitoring crop and supplies. Companies use drones to inspect installations in harsh and dangerous locations to identify damage to assets for example oil rigs, pipelines, bridges and heavy construction. Drones are also used in urban settings to inspect powerlines and roads, although managing a drone in this setting presents more challenges due to the impact on privacy which means tighter control is required to balance interests.

Other Related Technology

The following two technologies raise similar issues to AI and have particular application in the field of development.

Geospatial technology are technologies used in geographic mapping and include Geographic Information Systems (GIS) data analysis which is mapped on the basis of a georeferenced location; Global Positioning System (GPS) uses a network of satellites providing precise coordinates for the location of users; Remote Sensing (RS) is the capture of images from satellites and airborne cameras; and software such as Microsoft Virtual World and Google Earth. The layers of geographical, temporal and spatial data obtained can be used in the fields of medicine, conflict, environment, poverty reduction, agriculture, and others.

Nano-Technology is a technology which works at the nanoscale (1-100 nanometres). Applications include, renewable energy, lighter and faster products, earlier diagnosis of diseases, electronics, manufacturing, and development of materials including smart materials with innovative properties. As such its different uses in emerging market economies can be potentially transformative for the development of industries, including energy, health, and agriculture amongst others.

The legal framework applicable to these technologies will obviously depend on how they are deployed. However, issues of data ownership and access often arise with respect to geospatial technologies, which may have a national sovereignty dimension; while privacy and data protection laws will be applicable where the monitoring of peoples is concerned. For nano-technologies, environmental and safety concerns are sometimes raised, as well as the need for robust intellectual property regimes.

Legal and Regulatory Considerations for AI

Whilst AI remains in its infancy, the adoption of AI specific laws or regulations is likely to be premature. Existing regulators are best placed to assess the impact and needs of their specific sector mandate. For instance, controlling the use of personal data is key for public acceptance of AI adoption and development and so data protection regulations should be applied to AI powered technologies.

[21] NIKKEI Asian Review, "Toshiba taps AI to boost productivity at memory plant," June 29, 2016. http://asia.nikkei.com/Tech-Science/Tech/Toshiba-taps-AI-to-boost-productivity-at-memory-plant

Until the law itself is developed specifically for AI, a principles-based approach to regulation may be the best way forward. This is the approach of IBM who has proposed three principles: [22]

1. Purpose: to assist not replace humans.
2. Transparency: how platforms are trained and what data is used in the training.
3. Skills: AI must be developed with industry people (doctors, teachers, engineers, lawyers, accountants, underwriters) and companies must invest in the training of human workers.

This final skills principle seeks to avoid structural unemployment where industry professionals lose their jobs to AI. It also provides the necessary technical capacity to those working in the sector.

In the UK, the House of Lords Select Committee on Artificial Intelligence in their report[23] proposes a cross-sector ethical AI code and as a starting point proposes 6 principles:

1. Artificial intelligence should be developed for the common good and benefit of humanity.
2. Artificial intelligence should operate on principles of intelligibility and fairness.
3. Artificial intelligence should not be used to diminish the data rights or privacy of individuals, families or communities.
4. All citizens have the right to be educated to enable them to flourish mentally, emotionally and economically alongside artificial intelligence.
5. The autonomous power to hurt, destroy or deceive human beings should never be vested in artificial intelligence.

The transparency of algorithms is an important question which has already emerged as a policy concern. Algorithms are generally valuable intellectual property assets and as such may be kept hidden from public view, which may clash with demands for transparency and accountability. Legal regimes and regulatory mechanisms need to be implemented that offer a means of reconciling these potentially conflicting interests.[24]

The issues arising out of flying drones relate to the aviation industry, the safety of those in its flight path, as well as privacy and data protection issues and cybersecurity. Whilst certain drone usage should be regulated, this need not be in the same manner as traditional airplanes.[25] Overtly strict, burdensome or ill-suited rules could impede the deployment of drones in emerging market economies.

Cloud Computing

Cloud Computing is a natural enabler of disruptive technologies, by offering on-demand, scalable and location independent computation services, which allow dispersed technologies to communicate, share, gather and store data, information, assets, payment and a range of other actions. The 'cloud' market can be broadly distinguished into three levels of service: infrastructure as a service (IaaS); platform as a service (PaaS); and software as a service (SaaS). In addition, there are public, private, hybrid and community cloud deployment models. In a public cloud the resources are shared ('multi-tenanted') with virtual machines separating the resources of the different users. This model allows users to take advantage of economies of scale. In contrast

[22] https://www.ibm.com/blogs/think/2017/01/ibm-cognitive-principles/

[23] House of Lords, Artificial Intelligence Committee, AI in the UK: ready, willing and able? Report of Session 2017-19 - published 16 April 2017 - HL Paper 100, available at: https://publications.parliament.uk/pa/ld201719/ldselect/ldai/100/10002.htm

[24] In terms of what is needed to both promote and control AI development see the following paper which also refers to strategies deployed by China, Singapore, Japan, South Korea, USA, Canada and European countries. The Age of Artificial Intelligence towards a European Strategy for Human-Centric Machines, European Political Strategy Centre Note, Issue 29 27 March 2018. https://ec.europa.eu/epsc/sites/epsc/files/epsc_strategicnote_ai.pdf

[25] The UK Civil Aviation Authority has a number of useful documents considering the regulated use of drones: https://www.caa.co.uk/consumers/unmanned-aircraft-and-drones/

a private cloud is used exclusively by one user, meaning that the user has greater control over security protocols. There are also hybrid clouds where some resources are held on a private cloud and other resources on a public cloud.

> "Cloud computing, "the cloud", involves cloud service providers (providers): those offering the service, provisioning and managing a set of technical resources, among tenants: those consuming the cloud services through direct relationships with providers. The providers' business model is generally to leverage economies of scale by sharing resources between tenants, while tenants gain from being able to pay only for the resources they require, thus removing a costly start-up base and being able to acquire service elasticity—to rapidly scale up and/or scale down resources in response to fluctuations in demand—and more generally, improving access to storage and computational services. The end-user of a system may interact with a cloud provider either directly or indirectly via tenant provided services."[26]

The uses and application of Cloud Computing technology are endless and interrelated with all other disruptive technologies considered in this paper.

Legal and Regulatory Considerations for Cloud Computing

Cloud Computing is another case of where the broader legal framework will vary depending on the context of its application. What will also determine the legal framework for a cloud is whether it is for private use or public use.

On the issue of location independency, there may be limitations due to a range of considerations. Firstly, providers may opt for a local cloud to store their content due to the laws of physics, i.e. the need for speed. Secondly, there may be content licensing laws (private law) which dictate the location and availability of data. Third, legislation or regulation may also specify the location of data, e.g. in Russia and China user data must be stored on servers located domestically. The implications of location independence include difficulties of enforcement against remote entities, as well as the potential for conflicts of law for both users and service providers.

To facilitate public sector adoption of Cloud technologies, data classification may be key, distinguishing national security data from open or publicly accessible data as required under freedom of information laws.[27] Data protection and cybersecurity rules will also be relevant, alongside other use specific obligations.

Standards

Cloud computing is a good example for setting out the relevance and importance of standards in the regulation of disruptive technologies. It is important to appreciate that there is no single global standard setting body, with standards being developed as quickly as innovations emerge. Standards are developed by different types of bodies, both de jure (e.g. ISO) and de facto (e.g. IETF) organisations, operating at national, regional and international level, or emerge from market practice. It is important to map those most applicable to the circumstances at hand.

There are broadly three categories of standards:

[26] Jatinder Singh, Thomas Pasquier, Jean Bacon, Hajoon Ko, and David Eyers, 'Twenty security considerations for cloud-supported Internet of Things', *IEEE Internet of Things Journal*, Volume 3, No.3, June 2016, p.270

[27] See Kingdom of Saudi Arabia, *Cloud Computing Regulatory* Framework, Communications and Information Technology Commission (February 2018)(http://www.citc.gov.sa/en/RulesandSystems/RegulatoryDocuments/Pages/CCRF.aspx). See also Gleeson and Walden, 'Placing the state in the cloud: Issues of data governance and public procurement', *Computer Law and Security Review* 32 (2016)

Technical standards – specify the "gory details" of a format, protocol, or interface and describe how to make things works in an interoperable manner. For example, in cloud computing technical standards cloud be used to define interoperable interfaces between different cloud providers.

Informational standards – set the parameters for types of information or metrics that can be used to communicate information about a product or service. Guidelines on "standardised" attributes for cloud Service Level Agreements (SLAs) have become a focus for a variety of bodies involved in cloud standards. Organisations have focussed on standardising SLAs to provide meaningful comparisons between, and evaluations of, competing cloud vendors.

Evaluative standards – tests and certifies the proper use of best-known practices. They are seen as a means of enabling cloud users to assess service providers and their service quality including, for example, uptime, performance, availability, security, privacy, compliance, and portability across cloud providers. Unlike technical standards, where compliance can be measured objectively, evaluative standards often depend on third-party certification to demonstrate compliance.[28]

These standards can be developed by public or by private actors. Public standards will normally be enrolled as part of the legislative or regulatory framework, not always directly legally binding, they may gain justiciability through their relationship with the state law. Private standards will normally arise through a contract, or through a certification scheme (which may have statutory backing), or a private standard setting organisation.

> Standards serve a multitude of different purposes, whether solving a technical problem; enabling interoperability; facilitating competition, or as a means of generating a trusted environment. The greater the degree to which a standard is developed to address, or becomes associated with, a public policy purpose (external), rather than an industry purpose (internal), the greater the likelihood that the standard will have legal effect, whether expressly sought or achieved through public or private law mechanisms.
>
> The standards-making process will also generally differ between technical, informational and evaluative standards. The institutional structure within which technical standards are developed varies considerably from official to private, and formal to ad hoc arrangements; reflecting the diverse nature of the industry. By contrast, informational and evaluative standards will usually involve a broader range of stakeholder participants, either at the drafting stage or through consultation mechanisms designed to elicit input from interested or affected parties. Governance and accountability concerns are also more likely to arise in the development of informational and evaluative standards, reflecting their potential legal role.
>
> *Extract from, Gleeson and Walden, 'It's a jungle out there'?: Cloud computing, standards and the law*

In the early days of cloud computing, whilst governments struggled to comprehend the technology, it was in fact market players who developed and adopted industry standards. The impetus came from the desire to ensure that consumer confidence was maintained, but also to distinguish themselves from those companies who did not offer a service which met certain minimum standards related to data protection, security, accessibility and integrity.

Existing standards may also act as impediments to emerging market economies where the concerns are different to those of developed countries. Whilst the principles may remain the same, bespoke standards may need to emerge that better reflect the environment and culture of a particular country or region. In this context it is worth noting, Microsoft's policy recommendations in its 'Cloud for Global Good' roadmap which fall under the headings: trusted; responsive; and inclusive cloud.[29] Also the policy areas used in the BSA Global

[28] Gleeson and Walden, 'It's a jungle out there'?: Cloud computing, standards and the law', *European Journal of Law and Technology* Volume 5, No 2 (2014), p.8

[29] Available at: https://news.microsoft.com/cloudforgood/

Cloud Computing Scorecard which ranks countries' preparedness for adoption and growth of cloud computing services: Data privacy; security; cybercrime; IP rights; support for industry-led standards and international harmonization of rules; promoting free trade; and IT readiness and broadband deployment.[30]

The Internet of Things

The Internet of Things has many uses which have become integral to our daily lives. The devices that comprise the Internet of Things can sense, act or do both.

> "The world of the 'Internet of Things' ('IoT') is just one manifestation of recent developments in information and communication technologies ('ICTs'), closely tied to others, including 'cloud computing' and 'big data'. For our purposes, the 'Thing' in the IoT is any physical entity capable of connectivity that directly interfaces the physical world, such as embedded devices, sensors and actuators". This contrasts with other definitions that extend to virtual things, as well as physical, and can encompass the user.[31]"

IoT devices rely on communication between 'things' and the Cloud in a bidirectional flow, meaning that security and proper management of data and identity is critically important.

The uses of IoT include anything from smart homes to smart cities, smart grids, smart supply chains, smart farming, smart roads, environmental monitoring and natural disaster prevention, smart water (supplies and pollution), logistics, industrial control, energy, personal health wearables, crime detection, elderly care, and the list continues. An application of IoT in the public sector is the programme to digitise the 800 year old Port of Rotterdam using IoT, Weather Company and IBM's Watson.[32] Another is an Italian local social services for the elderly initiative in the City of Bolzano which monitors the habits of the elderly in their own homes looking for out of the ordinary events to direct social care where needed.[33]

Legal and Regulatory Considerations for IoT

The applicable legal framework will involve considerations of cybersecurity and data protection, while wider issues will include the nature of the legal relationships and liabilities of the various parties within the IoT ecosystem, including contract law and consumer protection rules.[34]

The reliance of most IoT ecosystems on the Cloud raises security concerns for all actors including end users, cloud providers and tenants and relate to confidentiality, integrity and availability. Six broad concerns have been identified:

1) Issues of data transport to/from cloud services and data management in the cloud;
2) Issues associated with identity management;
3) Issues associated with the scale of IoT;
4) Issues arising from malicious "things";
5) Issues of certification, trust, and compliance with regulations and contractual obligations;

[30] http://cloudscorecard.bsa.org/2018/

[31] See respectively, ITU-T Recommendation Y.2060, Overview of the Internet of Things (06/2012), at 3.2.3, which includes virtual things, and ISO/IEC JTC 1, Internet of Things (IoT). Preliminary Report 2014, 2015, at 4.1, which infers that persons are included within the definition.

[32] For more information see: https://www.ibm.com/blogs/industries/building-the-worlds-smartest-port/ and https://www.portofrotterdam.com/en/news-and-press-releases/port-of-rotterdam-teams-with-ibm-internet-of-things-to-digitize-operations

[33]

[34] See Kuan Hon, Millard and Singh, 'Twenty Legal Considerations for Cloud of Things', available at SSRN: https://ssrn.com/abstract=2716966

6) Issues arising from further decentralization into multiple clouds, fog services, etc.[35]

Governments are currently looking at the creation of a standardised set of cybersecurity standards for the IoT specifically.[36]

When it comes to the IoT, there are also the questions of how informed a user's consent or transparent the 'layers' of legal agreements are, especially when each 'smart thing' involves numerous agreements governing the IoT as a product, service and software, as well as its interaction with the user, the chain of service providers and other IoT devices.[37]

Blockchains

A Blockchain is in effect a database which uses cryptographic functions to maintain data integrity and identity authentication. It covers distributed and centralised ledger technologies, as well as crypto-currencies. A ledger tracks transaction, while a distributed ledger is one which uses a decentralised P2P network to maintain the ledger. The original use for blockchains was bitcoins, a crypto-currency which operates in a "trustless environment" meaning that the users do not need to trust one another, instead the users rely on the technology.

As with other technologies, blockchain has evolved through different generations, of which the following merely summarises the highlights. The first generation blockchain was developed in 2009 by Satoshi Nakamoto for use with the Bitcoin, it was an open permissionless system. Thus the original usage was for a decentralised currency governed by protocols, not a central entity.[38] In 2014 Vitalik Buterin introduced the second generation blockchain, Ethereum with smart contracts forming the basis. This platform led to the development of decentralised apps beyond bitcoins.[39] A third generation focuses on applications beyond money, to develop interoperable ecosystems based on distributed ledgers.[40] There is talk of fourth generation blockchains which can be used in more complex environments with a focus on scalability and speed through the use of a Crypto Relational Database.[41] As the blockchain technology develops from currency to smart contracts and beyond, the issues of privacy and scalability become clearer. The latest generation blockchain technologies try to resolve this through different means, including the use of centralised platforms.

A distributed storage network means that the blockchain is not stored by a single central party, but distributed across a number of nodes, which each hold a copy of the ledger. Blockchains can be either open access, permissionless systems, or closed access, permissioned systems.[42] Open access systems can operate in a

[35] These broad concerns are taken from the paper which details the twenty questions to be considered, Singh, et al, Twenty Security Considerations for Cloud-Supported Internet of Things, IEEE Internet of Things Journal, Vol. 3, No. 3 June 2016

[36] A recent report is that by the National Institute of Standards and Technology, NIST Interagency Report (NISTIR) 8200, Status of International Cybersecurity Standardization for Internet of Things (IoT), 2018. Available at: https://csrc.nist.gov/publications/detail/nistir/8200/draft

[37] See: Noto La Diega, & Walden. "Contracting for the 'Internet of Things': looking into the Nest." *European Journal of Law and Technology*, 7.2 (2016)

[38] See: Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf

[39] See: What is Ethereum? A Step-by-Step Beginners Guide. https://blockgeeks.com/guides/ethereum/

[40] See: Vinay Gupta, A Brief History of Blockchain. https://hbr.org/2017/02/a-brief-history-of-blockchain

[41] See: https://news.bitcoin.com/pr-multiversum-delivering-4th-generation-blockchain-a-crypto-relational-database-pre-ico-raises-2-9million-in-just-6-days/

[42] Bacon, Michels, Millard and Singh, Blockchain Demystified (December 20, 2017). Queen Mary School of Law Legal Studies Research Paper No. 268/2017. Available at SSRN: https://ssrn.com/abstract=3091218

trustless environment. Closed environments can use either a central or a number of smaller nodes acting as trusted intermediaries to control the blockchain. Blockchains can have localised or global application, be public or private platforms. The identity of the participants can either be pseudonym-based using a public key infrastructure (PKI) to create a digital signature or real-world identity based. The identity used is important if using a public platform from where the blockchain archive can be downloaded by anyone.

What creates trust is the immutable nature of the ledger. Each entry is timestamped with a hash unique identifier mathematically generated and where distributed, it is replicated across all nodes. This means that were a single user to either amend or delete an entry it would be noticeable to everyone.

Cryptocurrencies

Cryptocurrencies have emerged as a sub-category of digital or virtual money systems. As mentioned above, they are based on trust and markets, rather than legal recognition and central government oversight. They offer low cost, efficient, fast alternatives to traditional money with an inbuilt blockchain safeguard. At the same time, the technology is complex and most users will lack a complete understanding of how they work and of the associated risks. The sheer scale of cryptocurrency value also means that they could impact on the financial stability of the economy and as such cannot be ignored by governments. The difficulty is that they have not generally be backed by central banks nor regulated by financial authorities. Their distributed control and transnational operations may also raise collateral issues such as money laundering and use in 'dark' markets.

Smart Contracts

Smart Contracts are automated contracts. Some say they will replace the need for lawyers to draft and seek enforcement. Others are more cautious as to whether they can truly replace the need for a human drafter or dispute resolver. The reality will likely lie somewhere in between. Technology currently relies on a human inputting legal contract terms in computer code, and lawyers are still needed to negotiate more complex contracts. Thus, it will take time before a smart contract itself reaches a level of sophistication where it can fully self-generate and self-execute.

Smart contracts operate on a blockchain protocol and form the contractual agreement, as well as governing the protocols necessary for the fulfilment of contractual obligations. The self-executing ability of smart contracts is what distinguishes them from electronic agreements and also means that disputes can be limited – it is also what makes them smart. For example, no reliance needs to be placed on the debtor to pay for goods received. The smart contract will itself allocate the digital assets once the goods are received. It is evident that the use of smart contracts can impact on electronic commerce, online agreements, and online dispute resolution (ODR). The technology used by smart contracts means that ODRs can be enforced without needing to rely on the national courts, since the digital assets can also be held by the smart contract.[43] Importantly there is no need to trust a party or rely on a third party, the code enforces everything. For this reason, the code needs to be trusted to be secure and functional. Smart contracts are based on conditions agreed by the parties and so are legally binding, which links back to Lessig's assertion that "code is law".[44] This clearly highlights the risks associated with smart contracts which is that the coding could lead to faults, mistakes or unintended consequences.

[43] For more on ODRs and the implications of smart contracts on law see: Riikka Koulu 'Blockchains and Online Dispute Resolution: Smart Contracts as an
Alternative to Enforcement' (2016) 13 SCRIPTed available at: https://script-ed.org/article/blockchainsand-online-dispute-resolution-smart-contracts-as-an-alternative-to-enforcement/

[44] Lawrence Lessig Code and other Laws of Cyberspace (1999).

When it comes to enforcement of contracts, in permissionless platforms, dispute resolution mechanisms can be built into the contract or delegated to an arbitrator. In permissioned platforms, arbitration decisions or remedies can be added to the smart contract.

Other Uses

Beyond crypto-currencies, blockchains are being used by banks, governments, jewellery companies[45] and industries such as the cotton trade to record the supply chain of a product[46] and the largest shipping logistics company Maersk, which handles 30 million shipments a day with each shipment generating 30 documents.[47] It is here where innovations for uses in emerging market economies will spring up. In combination with Big Data and AI, blockchains can be useful for government planning, for example in budget planning, redirecting funds to an area which needs it most from another area which may operate a surplus. Blockchain and ledger technologies can also be used to limit the potential abuse of public funds, conducting a smart reconciliation.

Blockchains are increasingly being used as permissioned, closed platforms to assist companies, organisations and even governments to centralise data, processes, and services. These are not used only in commercial contexts but also humanitarian, aid and development projects. For example, blockchain technology is used in the ID2020 initiative which seeks to provide identification to the 1.1 billion people who currently live with no officially recognised identity.[48] This operates on a permissioned ledger which helps maintain both control and confidentiality.

> "Accenture, Microsoft and Avanade have built a sophisticated, permissioned blockchain which connects existing record-keeping systems from private and public institutions into one database. The result is a rich set of portable, personal credentials that have been validated by multiple trusted parties, such as birth registration data from UNICEF; national ID numbers or voter documents issued by national registration authorities or electoral commissions; vaccination records from GAVI (a global vaccine alliance) and other non-government organisations (NGOs); and refugee registration data from UNHCR. In practice, this means someone arriving at a border crossing could use the information stored on the blockchain to prove he or she originated from an area where they faced violence or persecution, or that they qualified for emergency assistance or aid. In their host country, the same person could call up their school records to help them find employment, or to find information on their medical history in the event of a health emergency".[49]

It can also be used to track and trace aid funding, such as money provided to an international organisation that then gives funds to a local NGO who then sends funds to local schools or clinics.

Legal and Regulatory Considerations for Blockchains

The multitude ways in which blockchains can be deployed obviously means that any legal response needs to be tailored to the circumstances. In terms of characteristics, it is important to consider how trust and control operate, whilst the early blockchains functioned in trustless environments, future blockchains will increasingly be trusted nodes with limited trusted parties having control over the ledger. Second, the visibility and identity

[45] A joint initiative between gold and diamond companies and IBM called TrustChain

[46] For example of its use to increase traceability in supply chains see Project Provenance Ltd, White Paper Blockchain: the solution for transparency in product supply chains, (2015) available at: https://www.provenance.org/whitepaper

[47] https://www.maersk.com/press/press-release-archive/maersk-and-ibm-to-form-joint-venture https://www.ibm.com/blogs/blockchain/2018/01/digitizing-global-trade-maersk-ibm/

[48] https://id2020.org/

[49] For further information on this and other uses see: the GSMA/Deloitte Paper, Blockchain for Development (2017), available at: https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2017/12/Blockchain-for-Development.pdf

of participants will impact the regulatory and legislative requirements. For example, questions to consider include:

(i) Who can propose new transactions to be added to the ledger;
(ii) Who stores a copy of the ledger;
(iii) Who can add new blocks to the ledger;
(iv) Who can view the ledger;
(v) Whether users are identifiable; and,
(vi) Who controls the platform's underlying software.[50]

While the use case will determine the specific legal and regulatory implications, three areas of law are worth highlighting as raising more generic concerns for blockchain technologies: data protection, issues of legal validity and evidential rules.

Under EU data protection law, the regime is applicable to both controllers and processors with a broad territorial scope. In terms of compliance, it is important to identify who determines the purposes and means of processing (i.e. controller) and who processes the data on behalf of others (i.e. processor). In distributed ledger models, the control is deliberately not centralised and raises a number of issues in trying to identify the controller and processor. Users themselves are more likely to be controllers, with nodes and miners being either the processors or controllers depending on how active a role they take with the transaction data. In terms of personal data, this includes pseudonymised data and in most instances there will need to be a link to a real-world identity to comply with legal requirements, such as anti-money laundering obligations. The uncertainty which surrounds the application of data protection laws will affect how data subjects enforce their rights, identification of who has controller and processor obligations will not always be clear and where there are joint responsibilities, platforms will need to either contractually determine individual responsibilities or through the use of standard terms. Uncertainty surrounding potential obligations, rights and liabilities may inhibit innovation.

A second area of concern is whether the legal acts executed through blockchain technologies have legal validity and are enforceable in a jurisdiction. For example, is a smart contract capable of being recognised as a contract in law? Common law countries are unlikely to have an issue since the principles of contract law are flexible enough to apply to new modes of contracting; however, civil law countries tend to have stricter legal requirements for the formation of valid contracts that may need to be revisited in the context of smart contracts.[51] In addition, laws and regulations may contain other form requirements that while not expressly prohibiting electronic means of doing business may create uncertainty about their validity, such as requirements that contracts be 'in writing', 'signed' or the need for 'originals'. There have been law reform initiatives at a national, regional and international level to address such issues, including the United National Convention on the Use of Electronic Communications in International Contracts (2005), which contains a provision directly applicable to smart contract:

> A contract formed by the interaction of an automated message system and a natural person, or by the interaction of automated message systems, shall not be denied validity or enforceability on the

[50] Taken from Bacon et al, Blockchains Demystified, QMUL, School of Law Legal Studies Research Paper (2017), available at: https://ssrn.com/abstract=3091218

[51] For a brief overview of several jurisdictions and the difficulties that may arise, see Can smart contracts be legally binding contracts? – An R3 and Norton Rose Fulbright White Paper, November 2016. Available at: http://www.nortonrosefulbright.com/files/r3-and-norton-rose-fulbright-white-paper-full-report-144581.pdf

> sole ground that no natural person reviewed or intervened in each of the individual actions carried out by the automated message systems or the resulting contract. (Article 12)

However, emerging economies tend to have more archaic and less flexible legal and administrative systems that may retain form requirements or practices that mean that blockchain transactions have uncertain legal status.

A related issue to consider in relation to smart contracts and blockchain implementations are national evidential rules. If the processes are digitised but electronic evidence is either not recognised, understood or trusted by judicial systems, then the value of the technology itself will be lowered. In The Gambia and Botswana, for example, electronic evidence is admissible, but only when the adducing party can certify that the computer which generated the evidence is 'operating properly'; a potentially problematic requirement in a distributed processing environment. The certification requirements will also go to the question of probative value or weight given to electronic evidence. In many Latin American countries evidence must be notarised by a third-party. The UNCITRAL Model E-Commerce Law,[52] sets out a provision to deal with admissibility of electronic evidence.

> Article 9. Admissibility and evidential weight of data messages
>
> (1) In any legal proceedings, nothing in the application of the rules of evidence shall apply so as to deny the admissibility of a data message in evidence:
> (a) on the sole ground that it is a data message; or,
> (b) if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form.
> (2) Information in the form of a data message shall be given due evidential weight. In assessing the evidential weight of a data message, regard shall be had to the reliability of the manner in which the data message was generated, stored or communicated, to the reliability of the manner in which the integrity of the information was maintained, to the manner in which its originator was identified, and to any other relevant factor.

These international instruments are a good starting point for reforming or introducing both E-Commerce laws and rules on admissibility of electronic evidence.

FinTech

FinTech is the term used to describe the development of technology for use in finance. It is one area where the transformation of a sector by technology is visible in daily life. It has reshaped the way people pay, invest, insure, manage assets, do business and has also created new money. This technological innovation can be seen in both emerging market economies as well as developed economies, from the M-Pesa, a mobile money transfer service in Kenya, to the variety of innovations available in crowdfunding and peer to peer lending platforms.[53] Fintech has also increased efficiency and transparency across the financial industry. Through the application of Fintech to the infrastructure of banks (where by the cloud and mobile technology consolidate

[52] UNCITRAL Model Law on Electronic Commerce (1996)

[53] In 2013, the World Bank's Report 'Crowdfunding's Potential for the Developing World' was published on the new frontiers of global technology such as rewards-based crowdfunding. Available at: http://www.infodev.org/infodev-files/wb_crowdfundingreport-v12.pdf
The growth of P2P lending and crowdfunding in emerging market economies is demonstrated by China-based Demohour which provides a reward-based platform for Chinese businesses, and SeedAsia, which operates a pan-Asian equity crowdfunding platform for Chinese and Southeast Asian tech start-ups. Examples of African platforms include the South African rewards platform Startme, which funds both entrepreneurial and cause related campaigns, and P2P lenders Lendico and Zidisha.

internal and external data to a single place), it has the ability to increase the efficiency, usability and accessibility of traditional bank services. Fintech can also optimise investing through various innovations, including the use of robo-advisers and automated investment tools. When it comes to online automated Fintech offerings, issues of Know-Your-Client checks for anti-money laundering purposes will arise and it is important to ensure clear allocation of responsibility amongst the players.

Mobile money using your mobile phone to make payments is a good tool for enhancing financial inclusion and empowerment, by providing access to those without bank accounts. Since it relies on existing networks of agents to sell Mobile Money (normally a scratch card similar to airtime), it increases its speed to market and can optimise the business process. The user has to set up an account and their transactions themselves are protected with a PIN. M-Pesa's success is underpinned by its ability to provide a low-cost option for those working in urban areas struggling to get bank accounts, enabling them to send and receive money. It can also be used by individuals in conflict or dangerous parts of the world where traditional banks have no presence. It is a fast, convenient and efficient way by which to make (normally small) payments either to businesses or P2P.

Another example is M-Changa, a platform based in Kenya and Tanzania that allows people to use their mobile money to crowdfund projects.[54] The World Bank itself is currently supporting a project in Kenya to use blockchain technology to issue mobile phone-based bond, the M-Akiba, allowing individuals to invest small amounts of money.[55]

Legal and Regulatory Considerations for Fintech

Of primary applicability to FinTech will be laws and regulations which govern the financial sector. These will need to be reviewed to ensure that they are not overtly restrictive whilst still meeting the public policy objectives. They should not, without good reason, exclude non-traditional banks from offering financial services and as far as possible accommodate the offerings of FinTech innovations. As set out above, mobile money is a good example of non-banks, in this case telecommunication companies, offering financial services.

An interesting example of regulatory impediments is Nigeria. While the rest of Africa accounts for half of the 700 million global mobile money users and despite the large proportion of the Nigerian population who are financially excluded,[56] mobile money has not been as popular. Whilst some element could be reflective of cultural preferences, there is no doubt that the policy of the Nigerian Central Bank together with the unfavourable regulatory environment has inhibited expansion of mobile money.[57] This example highlights the importance of the regulatory environment in both enabling and inhibiting Fintech.

It is not only regulatory policies which may impede innovation, but also regulatory uncertainty. If authorities are not in a position to revise regulations to accommodate new technologies or business models then they can adopt enabling initiatives. These can be as simple as offering guidance to companies to see where potential

[54] Interesting examples of combining lending and donations, as alternative finance models, include Kiva, which has helped facilitate zero interest loans from lenders in developed economies to low-income entrepreneurs in emerging market economies, and GlobalGiving, a donation based platform. In this context, a number of platforms have been setup with the specific purpose of facilitating investment rather than donations from developed to emerging economies. EmergingCrowd, a London-based equity crowdfunding platform aims to provide retail investors in the UK the opportunity to directly buy shares and bonds in companies predominantly based in Africa. Similarly, the Sunfunder platform has experimented with offering investors an opportunity to invest in a diversified portfolio of off-grid solar projects in emerging economies and earn a financial return.

[55] See: http://documents.worldbank.org/curated/en/480001493487780823/pdf/ISR-Disclosable-P151816-04-29-2017-1493487765405.pdf

[56] 40.1 million people were financially excluded in Nigeria in 2017 IFC Paper, 'Digital Access: The Future of Financial Inclusion in Africa', May 2018

[57] Its policy is based on concerns about money laundering and also the fear of loosing control to private money.

compliance issues may arise or they can offer controlled environments where new products can be offered to test compliance (these are referred to as regulatory 'sandboxes').

In addition to regulatory authorities, self-regulation is facilitating the entrance of new technology. For example, in 2015 in the China, the Shanghai Financial Information Association (SFIA) was founded as the first self-regulating FinTech association in China. These associations can help establish a baseline for market entrance, develop industry standards, as well as drafting templates for agreements in line with regulatory requirements. This will be of particular use to new market entrants and smaller companies.[58]

In addition to the guides and standards set by specific Associations, there are also papers which summarise best practice, for example the Basel Committee on Banking Supervision's Paper on Implications of FinTech developments for banks and bank supervisors.[59] With the blurring of boundaries between actors, activities and jurisdictions, caused by new technologies, such transnational approaches are crucial, for the effective regulation of all technologies. Other papers highlight issues for consideration, such as the IMF Staff Discussion Note on FinTech and Financial Services: Initial Considerations.[60]

Once it is acknowledged that an issue exists, there is a wealth of material which can be mapped and consulted to assist in the formulation of appropriate regulatory responses to the emergence of FinTech.

Collaborative Economy

Disruptive technologies have the potential to spur development through innovation in a multitude of areas and at all levels: Business to Business (B2B); Business to Consumer (B2C); Government to Consumer (G2C); and Peer to Peer (P2P). The levels are largely self-explanatory, however with the growth of the P2P economy, also known as the shared economy or the Collaborative Economy, the line between B2C and P2P is increasingly being blurred.

The Collaborative Economy uses online platforms to connect supply and demand for a product or service. In itself it is an innovative way to use technological advances and includes services in sectors such as food (Deliveroo, Feastly); goods (ebay, Etsy, Amazon), money (crypto-currencies, money-lending, crowdfunding); space (AirBnB, HomeAway, work space), transportation (Uber, Halo, Lyft, vehicle lending), and services (Task Rabbit). The apps or online presence, together with the digital payment systems provide consumers with speed, efficiency, usability, and a sense of security. The environment within which they operate creates its own private law rules (consented to with a click), specified dispute resolution mechanisms and features that facilitate trust (online reviews). Whilst such platforms are unquestionably enablers, they have also been used by companies to avoid liabilities under tax, labour and consumer protection laws.

One issue to note is a new breed of suppliers in the marketplace, the 'Prosumer'. A Prosumer is a hybrid Professional and Consumer, they fall short of a professional/business whilst supplying a good or service. These can be found on platforms such as AirBnB, an individual who advertises on the platform the availability of a spare room in their place or one of their properties. The platform helps match the room with an individual who is searching for a place to stay. The platform itself has no interest in the room (asset), nor does it set the price or availability of the room which are all controlled by the prosumer who owns the room. At the other end of the spectrum we have platforms such as Uber who may not own the car (asset), but they do set the

[58] Further detail on this and other concerns can be found in the White Paper produced by the World Economic Forum's Global Agenda Council on the Future of Financing & Capital, The Complex Regulatory Landscape for FinTech: An Uncertain Future for Small and Medium-Sized Enterprise Lending, August 2016.
[59] Sound Practices, February 2018. This paper considers implications and related considerations.
[60] SDN/17/05, June 2017 The focus of the paper is on FinTech for Cross-Border Payments, however it also provides a useful overview of the regulatory framework and implications.

price of the trip, the route and also allocate rides to drivers – most of this is done using sophisticated algorithms which belong to the platform (not its users). Whilst the algorithms are not publicly available, they determine the availability and price presented to the consumer. Whilst trust is placed in the algorithm, these are written by humans for businesses who want to maximise their profits. Consumer protection may not always be visible. For example, an algorithm can be set to increase the price of a taxi ride where the battery of the user's mobile is low. A way to resolve and increase transparency could be to make public the criteria used, whilst preserving the secrecy of the algorithm itself. Uber, Deliveroo and other similar platforms are closer to B2C then P2P.[61]

The Collaborative Economy has potential use in emerging market economies, providing opportunities for individuals to engage with the global economy. They can sell their products on platforms such as Ebay, Etsy or others, they can also raise funding through crowdfunding or peer to peer lending platforms.

Legal and Regulatory Considerations for the Collaborative Economy

The regulation of the Collaborative Economy, is complex, its uses cover an array of economic activities and do not always fit within existing legal categories. For these reasons, no consensus has been reached as to the best way to regulate the Collaborative Economy which analysts say is the fastest growing economy model[62] and which has a role to play in the growth of emerging market economies. Relevant legal issues which both enable and inhibit include data protection, intellectual property, and cybersecurity.[63] More broadly we have already seen that other laws are applicable to these platforms, such as, competition law, consumer protection (including market access and contract law), Labour laws, contract law, tax laws and dispute resolution. Collaborative funding platforms will also be subject to financial law and financial regulation.

General Legal and Regulatory Framework

For the purposes of this paper, the legal framework refers to primary and secondary legislation, substantive and procedural rules, judicial decisions and precedent. The regulatory framework may mean a regulator governing vertical sectoral activites (such as finance) or horizontal conduct (such as data or consumer protection), who operates through ex ante measures (e.g. licensing, authorisations or notifications) or ex post oversight (e.g. investigative powers, enforcement measures, audit and prosecution). On some aspects, regulators generally have more flexibility then the black letter law, as well as greater expertise then the legislator. Independence of the regulator is key to effective and fair implementation and enforcement of the regulations. Independence is required not only from the regulatees, but often also the government. We will touch on how government policy and actions can influence the development of these.

The legal and regulatory framework applicable to disruptive technologies is not a standard one, the technology, or even the precise use of a technology will dictate which laws are engaged. Due to the countless

[61] Uber has been the subject a different litigation across the world. In the UK the litigation focused on the status of the Uber drivers which the company defined as self-employed. The courts held that the drivers fell within the definition of workers meaning that in addition to being entitled to certain employment rights, Uber was also liable to pay taxation. This is an example of where platforms are used with either uncertainty as to the applicable regulations, or used to circumvent obligations.

[62] A study by PWC for the European Commission found that in UK on-demand household services, which could see revenues expand at roughly 45% a year to 2025. Whilst across Europe the collaborative economy accelerated generating revenues of €3.6bn and facilitating €28bn of transactions in 2015 in five sectors P2P accommodation, P2P transportation, On-demand household services, On demand professional services, collaborative finance. See PwC UK, (2014), Assessing the size and presence of the collaborative economy in Europe Available at: http://ec.europa.eu/DocsRoom/documents/16952/attachments/1/translations/en/renditions/native

[63] To see how the Collaborative Economy is being and could be regulated see, Vassilis Hatzopoulos, *The Collaborative Economy and EU Law* (2018)

permutations of technologies and uses, it is beyond the scope of this paper to comprehensively discuss all areas of law which form the applicable legal framework at any given time. Ultimately, laws need to be dynamic, law obtains its true meaning in its social, moral, economic and cultural consequences. The importance is to ensure that the law is relevant, effective and enforced.

This section will focus on laws with direct applicability to the technology itself such as cyber-security and related cybercrimes; data protection and access to information (this is also relevant to freedom of information and public authorities); and intellectual property.

Broader areas for consideration include Competition Law, Financial Law, Labour Law, Human Rights Law, Trade Laws, Contract Law, and Consumer Protection Laws, to name but a few. The World Bank will find that much of its existing guidance will apply to projects which make use of disruptive technologies. The aim of this paper is to highlight specific legal issues which may either enable or inhibit innovation and adoption of disruptive technologies.

When it comes to disruptive technologies, the legal and regulatory framework cannot rely solely on the laws of nation states but will inevitably include industry standards and platform/technology rules of engagement. So, beyond the laws set out, standards, guidelines and private agreements will need to form a key element of any legal advisory services.

Data Protection

Big Data, although not a technology in itself, is important for the economy, as well as almost every sector including development. In terms of its scale, it is predicted that by 2020 40 zettabytes[64] of data will have been created (in 2011 it stood at 1.8 zettabytes). Data is generated between people, between people and machines and between machines. Data is a valuable asset, as are the technologies which send, process and analyse data, including the database engines and applications. Big data analytics can generate insights at a speed, volume and variety not possible previously.

Together with other disruptive technologies, in particular AI and Cloud Computing, large, complex data sets can be processed in real-time. There is a range of uses, for example in the commercial sphere which includes analysing the market and increasing revenues and sales, innovation to develop or improve products including remote monitoring for efficiency and improvements, optimising production efficiency, supply chains, and delivery. In the financial sector, data can be analysed in real-time to forecast, conduct risk assessments and also prevent economic and financial crimes. In development it can be used to predict food and water shortages, weather, population movement, literacy levels, health issues, etc…

Since technologies either harvest, generate, process, analyse or use Big Data, it is something that governments, authorities and industries need to have in mind both in terms of regulating it but also using it in their work. This will raise directly issues of data protection and cybersecurity, whilst depending on the uses of the Big Data it could indirectly raise issues of competition law, constitutional law and even impact on the democratic process of states.

Big Data powers the economy including research and development.[65] With the increasing harvesting and use of data for personalised marketing, targeted advertising, newsfeeds and search results, there is an increasing

[64] 1 terabyte= 1000 gigabytes, 1 petabyte= 1000 terabytes, 1 exabyte= 1000 petabytes, and 1 zettabyte= 1000 exabytes

[65] For example the WB GSMA project which will work with mobile operators to use Big Data gathered from IOTs for development. See: http://www.worldbank.org/en/news/press-release/2018/02/26/world-bank-group-and-gsma-announce-partnership-to-leverage-iot-big-data-for-development

need for data to be protected. In addition to regulation of the data harvesting, processing and use, ethical principles and guidelines may also be used to control the use of Big Data.

Controlling the use and abuse of personal data in a Big Data environment is achieved through data protection laws and regulation. The European Union's General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679), which entered into force on 25 May 2018, sets out the scope, rights of data subjects, obligations of those who control or process data and supervision, liability, sanctions and remedies. In terms of obligations on controller's, the GDPR adopts two primary mechanisms that essentially place discretion upon the controller about the manner in which they comply with the GDPR: Data protection principles and risk-based decision-making:

Principles-based obligations

The GDPR lays down 6 principles relating to the processing of personal data: i.e. 'lawfulness, fairness and transparency', 'purpose limitation', 'data minimisation', 'accuracy', 'storage limitation' and 'integrity and confidentiality'. The controller has a general obligation to comply with these principles; as well as a 7th principle of 'accountability', which requires the controller to be able to demonstrate compliance with its obligations.

While each of the principles are elaborated in more detailed obligations in subsequent provisions, the general principles continue to be applicable where there are no specified requirements and obligations. As such, although a controller may operate in compliance with a specified obligation (e.g. data protection by design), its conduct overall could still be construed as being in breach of the general principle (e.g. data minimisation).

Risk-based decision-making

A risk-based approach to compliance means placing an obligation on the controller, in the first instance, to assess and evaluate the risks arising from each distinct processing activity and requiring it to vary its practices and procedures according to such an assessment. As a consequence, the controller has a degree of flexibility and discretion when making determinations as to the level of risk and what measures it should take to meet its compliance obligations.

In terms of enforcement in those areas where the controller must assess risk, while a regulator may disagree with the risk analysis carried out by a controller, the threshold for a regulator to make a finding of breach is likely to be higher where the controller has carried out the applicable risk analysis in good faith, taken into account all the known facts and circumstances and in accordance with regulatory guidelines or standard methodologies.

It is important that the substantial law provides a high level of protection whilst not making the obligations over burdensome to the extent that it makes no commercial sense to continue operations. Data security requires that there is integrity, confidentiality and availability. Under the GDPR, data subjects have the right to access, rectify, and erase their data. It is unlikely that the collection, transmission or processing of data will remain within the national borders of a single jurisdiction, thus laws and regulations will need to be in place to govern such cross-border elements.

Independent regulators

It is equally important to ensure that the procedural law and institutional mechanisms operate with integrity, independence, consistency and in accordance with clear and transparent laws. For example, on supervisory authorities, the GDPR states:

> (117) The establishment of supervisory authorities in Member States, empowered to perform their tasks and exercise their powers with complete independence, is an essential component of the protection of natural persons with regard to the processing of their personal data.

(118) The independence of supervisory authorities should not mean that the supervisory authorities cannot be subject to control or monitoring mechanisms regarding their financial expenditure or to judicial review.
(120) Each supervisory authority should be provided with the financial and human resources, premises and infrastructure necessary for the effective performance of their tasks, including those related to mutual assistance and cooperation with other supervisory authorities throughout the Union.
Each supervisory authority should have a separate, public annual budget, which may be part of the overall state or national budget.

Automation and design implications

Under Article 22 of the GDPR, special rules govern 'automated decision-making', where there is no human involvement, but the decision has a legal or similarly significant effect on a data subject. Such provisions will impact on the manner of deployment of a number of the disruptive technologies outlined above, such as blockchains, especially concerning the need for transparency and procedures to enable a right to appeal to a 'human in the loop' against such automated decisions. Similarly, requirements to operate in accordance with the principles of data protection by design and default (Article 25) has potential implications for the whole supply chain behind disruptive technologies and their deployment, reducing the use and abuse of personal data and enhancing cybersecurity.

While weak data protection law, regulation and protection may deter both companies and individuals when it comes to disruptive technologies, overly restrictive laws and enforcement can have a similar effect. When it comes to data protection, the law must be clear, while any obligations or restrictions must have a legitimate aim and be proportionate.

Cybersecurity

The relevance and importance of cybersecurity cannot be overstated. As more of daily life moves online, threats to individuals, companies and states originating online will also increase. In line with technological innovation, the sophistication of cybercrimes grow. Cybercrimes reflect a virtual version of ordinary crimes from child pornography, to fraud, theft and crimes of deception, or they facilitate ordinary crimes. But we need to be clear that there is a difference between cybersecurity (prevention) and cybercrimes (cure). The presence of cybercrimes in a legal system together with proper enforcement is an important deterrent that should form part of any legal framework. However, as with other crimes, prevention is better than a cure. The one issue to highlight here is that, particularly in emerging market economies with weak or compromised democratic institutions, the use of cybercrimes may be used to silence or control government opposition or criticism of government. This links into the need to ensure that countries have independent judicial and regulatory systems with enough power to conduct effective oversight over executive power. The Council of Europe's Convention on Cybercrime in 2001[66] or one of the other Conventions can be a good point to start when assessing cybercrime laws.[67]

Whatever role technology plays, cybersecurity must form a central element of any emerging digital economy. ISO/IEC 27032 defines cybersecurity as the "preservation of confidentiality, integrity and availability of information in the Cyberspace".[68]

[66] ETS No.185, 2001
[67] In this context refer to the Shanghai Coorperation Organization Agreement of Cooperation in the Field of International Information Security 2010; or the African Union Convention on Cyber Security and Personal Data Protection 2014; or the Commonwealth of Independent States Agreement on Cooperation on Combatting Offences Related to Computer Information 2001.
[68] ISO/IEC JTC1/SC27 IT-Security Techniques

Cybersecurity can be provided through the adoption of legislation, the establishment or extension of regulatory mandates, the training of public authorities, the education of both natural and legal persons, the adoption of cybersecurity strategies and the existence of skilled persons. Cybersecurity measures must ensure that assets are appropriately protected, whether they are tangible or intangible, belonging to companies, individuals or the state. It is important to distinguish between 'safeguarding' and 'notification' obligations. Safeguarding means implementing security measures, whereas the latter includes breach notifications and other forms of information sharing, which are important in the mitigation of harm.

A weak protection system will deter companies from either introducing their technologies into a jurisdiction or from investing in innovation because of high risks to their business and assets. If individuals do not feel protected they will be deterred from using the new technologies for fear of cyberattacks, vulnerabilities, identity theft and invasion of privacy.

Critical national infrastructures

Whilst adoption of Cloud based services by governments can offer benefits of scalability, resilience, security and cost efficiency, governments must ensure that their critical infrastructure services are secure. These include the national internet infrastructure, power grids, finance, health, and other infrastructures. It is considered best practice for states to adopt a National Cybersecurity Strategy with the aim of being able to respond to cyber-attacks or system failures.

Intellectual Property

Innovation in the information age creates intellectual property which is important for sustainable development acting as "the oil of the 21st century", as well as personal data.[69] It is therefore critical that the legal environment governing intellectual property rights should be robust enough to foster the long-term development and protection of intellectual property as a catalyst for sustainable economic development.

Intellectual Property law generally encompasses patent, trademark, design and copyright law. Intellectual Property provides an exclusive property right over an intangible asset, enabling the right holder to exclude other people from using the information without their authorisation. The premise of Intellectual Property is that without this exclusivity people would not create and disseminate new creations and inventions since the value of their creations could be too easily appropriated by others. The absence of Intellectual Property would arguably diminish any incentive to engage in further research and innovation.

Intellectual property rights are of crucial importance for modern businesses. This can be seen through the ever-increasing rise of intangible assets within the portfolios of companies. Copyrights and patents play an important role in industries which are research heavy, whereas brand value can be a very valuable asset and relies on trademarks.[70] Intellectual property rights not only serve to make research and development attractive but are also of increasing importance as a tradeable asset and as security for investment.

A strong understanding of how intellectual property law could be used and applied to innovation in technology, is necessary for sustainable development. Existing IP rules may not be fit in an environment where the AI machine 'invents' or 'creates' the IP. For example, it needs to be clear who the inventor/owner of the created IP is.

Intellectual Property policy is something that should be "tailored" to a particular state's or region's needs. This includes taking into account the level of national or regional development. A "one size fits all" approach cannot

[69] Mark Getty, CEO of Getty pictures, "Blood and Oil," The Economist (March 4, 2000), p. 68.
[70] See: Forbes most valuable brands list 2015 <http://www.forbes.com/powerful-brands/list/#tab:rank> last accessed: 22 April 2016.

be a viable option and careful drafting of Intellectual Property laws is required. For example, the World Trade Organisation's (WTO) Agreement on Trade Related Aspects of Intellectual Property Rights (TRIPS) does not set a model for Intellectual Property law. Instead it provides for minimum standards that the Intellectual Property legislation of WTO Member States should follow. TRIPS also provides flexibility to allow the tailoring of Intellectual Property law to better reflect domestic or regional needs.

Finally, it is also worth noting that strong IP protection can facilitate the growth and adoption of 'open source' solutions within disruptive technologies, e.g. software, hardware, data, by enabling enforceable private law contracts and licenses to be used to achieve alternative public interest objectives, such as greater access and interoperability.

Technology as a Solution

Technology does not only create the governance gaps or challenges for law and regulation, it can also be part of the solution.

RegTech

Technology can be used in any regulated sectors to conduct risk assessments, monitor, report and comply with regulatory obligations at reduced cost. This is known as 'RegTech'. In addition to digitalisation of reporting, technology can carry out automated compliance processes and checks, it can reduce operational risk, cybersecurity, and provide real-time analysis and compliance ('Compliance as a Service'), which in turn can be used to combat fraud and other crimes, as well as provide warnings on a range of other issues. Technology can include digital labour, robotic process automation, machine leaning, cognitive learning, big and smart data analysis, biometric technology, and natural language processing. RegTech does not negate the need for human input to update regulations and also to buy-in to the culture of regulatory compliance.[71]

Since 2015, the Financial Conduct Authority (FCA) in the UK been issuing calls for input on a range of issues in RegTech. In addition to the calls they also hold TechSprints, where participants are asked to develop a 'proof of concept',[72] this has included one which could make regulatory reporting requirements machine-readable and executable. As part of this initiative, BARAC[73] is currently investigating the possibility of using blockchain technology for automating regulation and compliance.

Globally there are already a number of RegTech companies providing solutions including for regulatory reporting (e.g. real time reporting), risk management (to detect compliance and regulatory risks),

[71] See RegTech in the cognitive era Insights from Gene Ludwig and Bridget van Kralingen, from the IBM Institute for Business Value, 2017. Available at: https://public.dhe.ibm.com/common/ssi/ecm/gb/en/gbe03845usen/global-business-services-global-business-services-gb-executive-brief-gbe03845usen-20170711.pdf

[72] More information on the calls, the TechSprints and the innovations to date can be found on the Authority's website at: https://www.fca.org.uk/firms/regtech

[73] http://blockchain.cs.ucl.ac.uk/barac-project/ According to the FCA, UCL and Santander are working on a project to use smart contract and distributed ledger technology to allow the FCA to verify compliance. The FCA has also worked with R3, RBS and another global bank to explore the possibility of using distributed ledger technology for regulatory reporting. The first stage of this programme was successful and will be used to inform the wider BARAC initiative. It is also worth referring to the FCA's Distributed Ledger Technology Feedback Statement on Discussion Paper 17/03, December 2017. https://www.fca.org.uk/publications/feedback-statements/fs17-4-distributed-ledger-technology

identification management (covering counterparty due diligence, KYC procedures and AML), compliance (real-time monitoring and tracking), and transactions (real-time monitoring and auditing).[74]

Privacy enabling technology (PET) can be integrated into technologies to protect privacy. Technologies can be used to enforce laws and standards. For example, blockchain technology is already being used in the arts to ensure that the owner of a work remains embedded into the image no matter how many times it is copied and pasted. The same traceability is being used in a range of other products, such as by Land Registries and for medical records.

Blockchain technology is already increasing the transparency and accountability of public authorities, as well as multinational companies. It is being used in accountability measures, for due diligence, and to certify supply chain compliance with laws, regulations and human rights.

Legal and Regulatory Approaches

> The fundamental premise of this data is that economic activity requires good rules and regulations that are efficient, accessible to all who need to use them, and simple to implement. Thus sometimes there is more emphasis on more regulation, such as stricter disclosure requirements in related-party transactions, and other times emphasis is on for simplified regulations, such as a one-stop shop for completing business startup formalities. Entrepreneurs may not be aware of all required procedures or may avoid legally required procedures altogether. But where regulation is particularly onerous, levels of informality are higher, which comes at a cost: firms in the informal sector usually grow more slowly, have less access to credit, and employ fewer workers - and those workers remain outside the protections of labor law. The indicator can help policymakers understand the business environment in a country and - along with information from other sources such as the World Bank's Enterprise Surveys - provide insights into potential areas of reform.[75]
>
> *World Bank Doing Business Project*

The above is particularly true for emerging market economies which often face the triangular need for political will, coordinated agency efforts and technical capacity for professionals including lawyers. When it comes to regulating technologies, the issue of uncoordinated agency efforts is a global problem; while in emerging market economies this is accentuated by the lack of access to information and digitisation of relevant laws and regulations, which means that conflicts will be identified a long way down the road.

In addition, there will often be a lack physical infrastructure to accommodate new technologies, with it being exacerbated by the lack of a legal infrastructure. For example, Africa has a good mobile network, however they often lack the high-speed internet required to power disruptive technologies. The reasons are partly funding, but also due to inefficient and ineffective licensing and regulatory regimes.

Local technical capacity is key for enabling policy, laws, and also sustainable development and local innovation. It is important for all stakeholders to have an understanding of the technology and its potential development. This includes members of the executive, the legislator and the judiciary, in addition to commercial practitioners and other professionals who may engage with technology. Together with training of

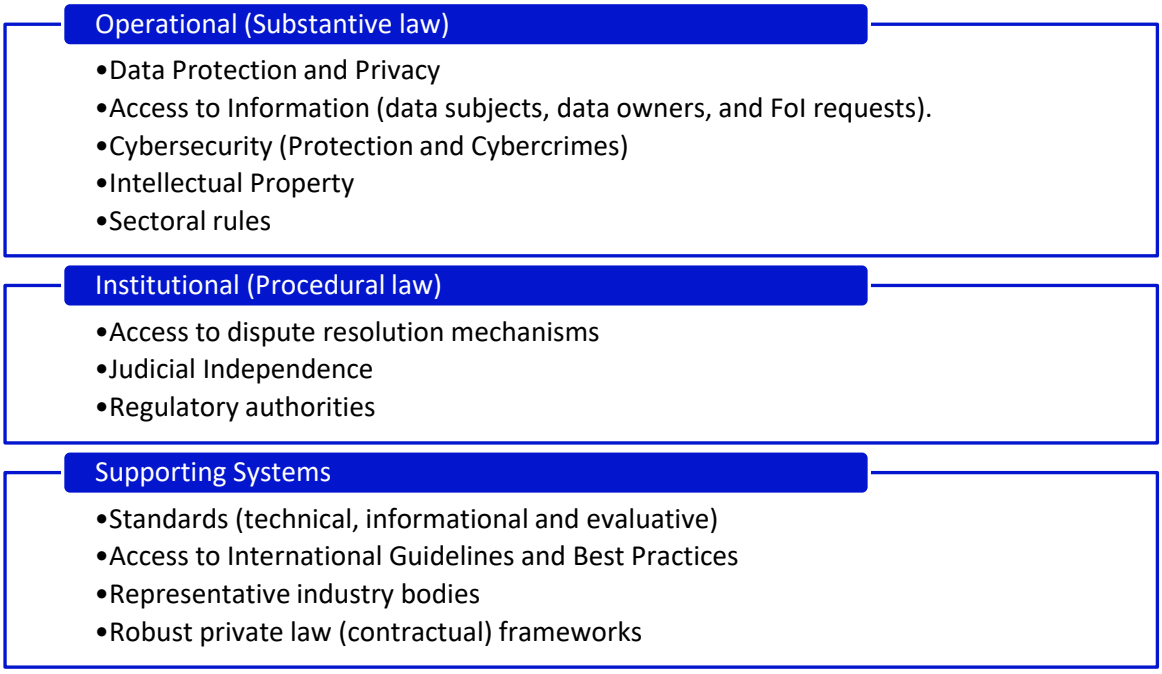
[74] Deloitte has established a RegTech Universe where they are compiling a list of RegTech companies along with the technologies and solutions they are offering. https://www2.deloitte.com/lu/en/pages/technology/articles/regtech-companies-compliance.html

[75] Taken from the World Bank Doing Business Project – Details from Strength of legal rights index/ Time required to enforce a contract (days)

professionals, there needs to be education of users and citizens not only about the technology but also issues such as privacy and cybersecurity.

Innovations in disruptive technologies will be generally be led by young and small start-ups, which is an indicator that project funding should also incorporate an element of facilitation and capacity building targeted specifically at the potential entrepreneur community. As well as creating a legal environment conducive to start-ups and more broadly new market entrants. This will be key to sustainability and continued innovation.

In summary three elements need to be considered: the operational, the institutional and supporting systems.



Regulatory uncertainty is an inhibiting factor for new market entrants. Regulators can adopt a number of enabling approaches and initiatives to alleviate some of this uncertainty. This includes regulatory sandboxes, greater and better co-operation between agencies and the provision of regulatory guidance to assist firms navigate the regulatory requirements.

Legislation and regulation requires flexibility to accommodate the variety of modes of innovation. For the foreseeable future it will need a largely a case by case approach with mutual oversight mandates held by different regulators. It is therefore important that clear lines of communications exist between the agencies, as well as agreed prioritisation of which will have priority to investigate, etc. One way to do this could be through joint committees, or the use of Memorandums of Understanding between agencies setting out the lines of communication, the process for mutual assistance and the prioritisation of action.

Regulatory sandboxes are something already in use in a number of countries including, Australia, Canada, Hong Kong, India, Korea, Malaysia, Singapore, Switzerland, United Arab Emirates, and the UK. They assist both the regulator and the regulated entity. These are where the regulator permits the testing of a new technology or business model in a controlled environment to see its compliance with regulatory requirements, but also to allow policymakers to see what changes the law and regulation requires to accommodate innovations.

Self and co-regulation can be particularly effective with new technology, particularly where companies are keen to gain and maintain trust and confidence from its users. However, if the private sector has insufficient incentives to regulate itself, state intervention will be required.

The discourse of globalisation means that legal reforms will often be unable to keep up with the pace of technological innovations. Therefore, in addition to the standards, guidelines and best practices, a supporting mechanism will be private law, in particular contractual agreements. Party autonomy and the freedom to contract is what keeps the global economy going round and should be recognised and protected. Contractual agreements mitigate the need to wait for legal reforms to create the requisite obligations, restrictions or rights. Contracts are not only used by the private sector but can also be used by the public sector, for example through public procurement procedures.

In addition to the substantive law, the procedural elements also need to be carefully established so as to ensure the greatest level of independence to the regulatory bodies free from government influence and a truly independent judiciary which can adjudicate on matters in accordance to the law and not politics. Consideration will need to be given to the process of appointments, the resources made available to a regulatory body or the judiciary, the mandate of the regulatory authority set out in legislation, and Constitutional protections of judicial independence.

When it comes to the institutional infrastructure, disruptive technologies and in particular blockchain technology can assist in combatting corruption (through the virtual trail created on the ledger), it can also reduce bureaucracy – although care needs to be taken to ensure that it is not merely accelerated but that it is actually minimised. For example, where verification processes can be conducted by the code, there would no longer exist the need for verification by officials.

An enabling environment is not only necessary for the private sector to innovate, it is of equal importance for the public sector to be able to take advantage of the innovations. What is imperative to create an enabling legal and regulatory environment for disruptive technologies is for political will to exist, for the appropriate physical and legal infrastructure to be in place and for technical capacity to be increased in all sectors, domains and at all levels.