



The Legal 500 Country Comparative Guides

Pakistan: Technology

This country-specific Q&A provides an overview to technology laws and regulations that may occur in Pakistan.

For a full list of jurisdictional Q&As visit [here](#)

Contributing Firm



RIAA Barker Gillette

Authors



Mustafa Munir Ahmed
Partner

mustafa.ahmed@riaabg.com



Saira Khalid Khan
Associate

saira.khalid@riaabg.com

1. What is the regulatory regime for technology?

The regime relating to the operational aspect of technology is primarily regulated by two regulators; (i) the Pakistan Telecommunication Authority (the “**PTA**”) established under the Pakistan Telecommunication (Re-organisation) Act, 1996 (the “**PTA Act**”) and; (ii) the Pakistan Electronic Media Regulatory Authority (the “**PEMRA**”) established under the Pakistan Electronic Media Regulatory Authority Ordinance, 2002 (the “**PEMRA Ordinance**”).

PTA has the mandate to regulate the establishment, operation and maintenance of telecommunication systems and the provision of the telecommunication services in Pakistan, which are regulated in terms of the PTA Act and the rules, regulations and guidelines framed thereunder (the “**PTA Laws**”).

PEMRA has the mandate to regulate the establishment and operation of all broadcast media and distribution services, which are regulated in terms of the PEMRA Ordinance and the rules and regulations framed thereunder (the “**PEMRA Laws**”).

2. Are communications networks or services regulated?

Pakistan Telecommunication Authority

The PTA is the regulatory body for the telecom sector in Pakistan and was established under the Pakistan Telecommunication (Re-organisation) Act, 1996. The primary functions of the PTA inter alia include the regulations of establishment, operation and maintenance of telecommunication systems and provision of telecommunication services in Pakistan.

For purposes of the foregoing:

(i) ‘telecommunication system’ includes, any electrical, electro-magnetic electronic, optical or optio-electronic system for the emission, conveyance, switching or reception of any intelligence within, or into, or from, Pakistan, whether or not that intelligence is subjected to rearrangement, computation or any other process in the course of operation of the system, and includes a cable transmission system, a cable television transmission system and terminal equipment; and

(ii) ‘telecommunication service’ includes, a service consisting in the emission, conveyance, switching or reception of any intelligence within, or into, or from, Pakistan by any electrical, electro-magnetic, electronic, optical or optio-electronic system, whether or not the intelligence is subjected to rearrangement, computation or any other process in the course of the service.

PTA is also responsible for dealing with applications relating to the use of radio-spectrum

frequency through its Frequency Allocation Board (“**FAB**”), which has the exclusive authority to allocate and assign portions of the radio frequency spectrum to the Government, providers of telecommunication services and telecommunication systems, radio and television broadcasting operations, public and private wireless operators, and others.

Pakistan Electronic Media Regulatory Authority

PEMRA is responsible for facilitating and regulating the establishment and operation of all broadcast media and distribution services in Pakistan established for the purpose of international, national, provincial, district and local or special target audiences. PEMRA regulates the distribution of foreign and local TV and radio channels in Pakistan.

For purposes of the foregoing:

(i) ‘broadcast media’ includes, such media which originate and propagate broadcast and pre-recorded signals by terrestrial means or through satellite for radio or television and includes teleporting, provision of access to broadcast signals by channel providers and such other forms of broadcast media as the Authority may, with the approval of the Federal Government; and

(ii) ‘distribution services’ includes, a service which receives broadcast and pre-recorded signals from different channels and distributes them to subscribers through cable, wireless or satellite options and includes Cable TV, LMDS, MMDS, DTH and such other similar technologies.

3. If so, what activities are covered and what licences or authorisations are required?

Pakistan Telecommunication Authority

No person, unless he has obtained a license from PTA, shall establish, maintain or operate any telecommunication system (as per item 1.1 above) or provide any telecommunication service (as per item 1.1 above).

Pakistan Electronic Media Regulatory Authority

PEMRA has the exclusive right to issue licenses for the establishment and operation of all broadcast media (as per item 1.1 above) and distribution services (as per item 1.1 above), therefore, any person desirous of operating broadcast media or a distribution service, shall be required to procure a license from PEMRA.

4. Is there any specific regulator for the provisions of communications-related

services?

Communications-related services in Pakistan can be broadly categorised into (i) telecommunication system and telecommunication services; and (ii) broadcasting media or distribution services.

The key regulatory body for telecommunications services in Pakistan is PTA, and FAB is part of PTA. PTA is a statutory body and is established under the PTA Act. The primary functions of PTA include:

- (i) Regulation, establishment, operation and maintenance of telecommunication systems and provision of telecommunication services in Pakistan, including but not limited to the grant and renewal of licenses, and the monitoring and enforcement of the terms thereof;
- (ii) Establishment or modification of accounting procedure for licences and regulate tariffs for telecommunication service in accordance with the PTA Act;
- (iii) Prescribing standards for telecommunication equipment and terminal equipment, certify compliance of such equipment with prescribed standards, and issue approvals of terminal equipment and of approved installers;
- (iv) Providing guidelines for, and determine, the terms of interconnection arrangements between licensees where the parties to those arrangements are unable to agree upon such terms;
- (v) To receive and expeditiously dispose of applications for the use of radio-frequency spectrum;
- (vi) To auction on such terms and conditions as PTA may determine from time to time, or other open transparent competitive process to determine eligibility for licensing FAB's allocated or assigned specific portions of radio frequency spectrum.
- (vii) To promote and protect the interests of users of telecommunication services in Pakistan;
- (viii) To promote the availability of a wide range of high quality, efficient, cost effective and competitive telecommunication services throughout Pakistan;
- (ix) To promote rapid modernization of telecommunication systems and telecommunication services;
- (x) To investigate and adjudicate on complaints and other claims made against licensees

arising out of alleged contraventions of the provisions of the PTA Laws;

(xi) To make recommendations to the Federal Government on policies with respect to international telecommunications, provision of support for participation in international meetings and agreements to be executed in relation to the routing of international traffic and accounting settlements; and

(xii) To perform such other functions as the Federal Government may assign from time to time.

The relevant government ministry vis-à-vis telecommunications services is the Ministry of Information and Technology and Telecommunication (the “**MOITT**”)

The key regulatory body for broadcasting media and distribution services in Pakistan is PEMRA, which is a statutory body and is established under the PEMRA Ordinance. PEMRA is responsible for regulating the establishment and operation of all broadcast media and distribution services in Pakistan established for the purpose of international, national, provincial, district, local or special target audiences. PEMRA also regulates the distribution of foreign and local TV and radio channels in Pakistan.

The relevant government ministry vis-à-vis telecommunications services is the Ministry of Information, Broadcasting, National History and Literary Heritage (Pakistan).

5. Are they independent of the government control?

PTA and PEMRA are controlled by the federal government whereby, the federal government may, as and when it considers necessary issue directives to the authorities on matters of policy, and such directives shall be binding on the authorities, provided that such directives are not in contravention of the PTA Act and/or the PEMRA Ordinance (as applicable), and if a question arises whether any matter is a matter of policy or not, the decision of the Federal Government shall be final.

6. Are platform providers (social media, content sharing, information search engines) regulated?

Generally, the above-mentioned platform providers (i.e. social media, content sharing, and information search engines) are not regulated. However, PTA being the telecom regulator in Pakistan, will implement policies to block websites with blasphemous, un-Islamic, offensive, objectionable, unethical, and immoral material. In this regard, PTA as and when directed by the Federal Government can direct/require its licensees to implement IP/URL blocking/filtering protocols.

Having stated the foregoing, whoever with dishonest intention (i) gains unauthorized access

to any information system or data, or (ii) and unauthorised access, copies or otherwise transmits or causes to be transmitted any data, or (iii) interferes with or damages or causes to be interfered with or damages any part or whole of an information system or data, or (iv) interferes with or damages, or causes to be interfered with or damaged, any part or whole of a critical information system, or data, shall be punishable with imprisonment, under the Prevention of Electronic Crimes Act, 2016 (the “PECA”).

It is pertinent to note that the provisions of PECA are not only specific to the licensees (including MNOs) of PTA but the scope of PECA extends to every citizen of Pakistan, wherever he may be, and also to every other person for the time being in Pakistan. The same also applies to any act committed outside Pakistan by any person; whereby the act constitutes an offence under PECA and affects any (i) person, (ii) property, (iii) information system, or (iv) data, in Pakistan.

For the purposes of the foregoing:

(i) The term ‘information system’ includes, electronic system for creating, generating, sending, receiving, storing, reproducing, displaying, recording or processing any information;

(ii) The term ‘data’ includes, any representation of fact, information or concept for processing in an information system including source code or a program suitable to cause an electronic system for creating, generating, sending, receiving, storing, reproducing, displaying, recording or processing any text, message, data, voice, sound, database, video, signals, software, computer programs, any forms of speech, sound, data, signal, writing, image or video, to perform a function or data relating to a communication indicating its origin, destination, route, time, size, duration or type of service.

Further, PECA provides that a service provider shall, within its existing or required technical capability, retain its specified traffic data (data relating to a communication indicating its origin, destination, route, time, size, duration or type of service) for a minimum period of one year or such period as PTA may notify from time to time and, subject to the production of a warrant issued by the court, provide that data to the investigation agency or the authorised officer whenever so required.

For the purpose hereof, a ‘service provider’ means to include a person who:

a) acts as a service provider in relation to sending, receiving, storing, processing or distributing any electronic communication, or the provision of other services in relation to electronic communication through an information system;

b) owns, possesses, operates, manages or controls a public switched network or provides telecommunication services; or

c) processes or stores data on behalf of such electronic communication service or users of such service.

Service providers are required to retain traffic data by fulfilling all requirements of data retention and its originality, as per the provisions of the PECA.

7. If so, does the reach of the regulator extend outside your jurisdiction?

The mandate of both PTA and PEMRA are geographically restricted to Pakistan, however as above, the scope of PECA extends to every citizen of Pakistan, wherever he may be, and also to every other person for the time being in Pakistan; the same also applies to any act committed outside Pakistan by any person if the act constitutes an offence under the PECA and affects any (i) person, (ii) property, (iii) information system, or (iv) data in Pakistan.

8. Does a telecoms operator need to be domiciled in the country?

The applicable law does not have a minimum domestic legal presence requirement. However, we note from experience that PTA prefers that a local entity (SPV) be established which applies for a license to provide telecommunication services. The SPV/local entity can be completely foreign owned/controlled.

9. Are there any restrictions on foreign ownership of telecoms operators?

Please refer to our response to item 2 above.

10. Are there any regulations covering interconnection between operators?

PTA has issued Interconnection Guidelines, 2004 (the “**Interconnection Guidelines**”), pursuant to which, all operators (licensees of PTA) are obliged to provide interconnection to other operators desiring to interconnect. Interconnection shall be permitted at any technically and economically feasible point. Where an operator submits its request for interconnection with another, the former is required to a response in writing. It may accept the request completely or partially. It can only deny the request in its entirety based on reasons which have been given fairly. The matter shall finally be subject to adjudication by PTA.

PTA shall publish all interconnection agreements submitted to it in such a manner as it may deem appropriate. However, the operators may request PTA to keep confidential any information or any section of an interconnection agreement, the disclosure of which would have the potential to seriously and prejudicially affect the operators. The decision to keep any such information confidential will be at the sole discretion of PTA.

11. If so are these different for operators with market power?

An operator shall be presumed to have significant market power when it has a share of more than twenty-five per cent of a particular telecommunication market. The relevant market for these purposes shall be based on sectoral revenues. PTA may, notwithstanding the foregoing, determine that an operator with a market share of less than twenty-five per cent of the relevant market has significant market power. It may also determine that an operator with a market share of more than twenty-five per cent of the relevant market does not have significant market power. In each case, PTA shall take into account the operator's ability to influence market conditions, its turnover relative to the size of the relevant market, its control of the means of access to customers, its access to financial resources and its experience in providing telecommunication services and products in the relevant market.

Any operator (licensee of PTA), who has been determined by PTA as an operator having significant market power ("**SMP**") is obliged to prepare and submit its Reference Interconnect Offer ("**ROI**") to PTA within one month of its determination as an SMP operator by PTA. The SMP operator shall make the ROI publicly available within seven (7) days after approval by PTA.

After the receipt of an interconnection request, both parties shall mutually negotiate interconnection terms and conditions, or adopt the RIO, as the case may be; the negotiations shall be completed as soon as possible but not later than 90 days from the date of the interconnection request.

Subject to the Interconnection Disputes Resolution Regulations 2004, an operator may file a claim with PTA, if such operator is unable to reach an agreement with the other operator:

a) on an interconnection arrangement; or

b) on a dispute arising out of a subsisting interconnection agreement, and such failure to agree continues for 60 days after the request for the interconnection arrangement was made or the dispute was raised; provided that, PTA may entertain a claim before the end of 60 days.

12. What are the principal consumer protection regulations that apply specifically to telecoms services?

PTA in exercise of its powers under the PTA Act has framed the Telecommunication Consumer Protection Regulations 2009 (the "**TCPR**") which is the principal consumer protection legislation that applies specifically to telecom service providers.

The highlights of the same are as follows:

(i) Ability of a consumer to choose an operator and service(s) as per their choice, including the provision of services to such a consumer on a fair, transparent, efficient, and non-discriminatory manner;

(ii) A Consumer to be provided with uninterrupted service, subject to certain technical exceptions;

(iii) Requirement of due notice in case of suspension, withdrawal or disconnection of service(s) by operators to a consumer;

(iv) Protections to a consumer against operators engaging in unfair commercial practices;

(v) Operator to disclose to end users the price, terms and conditions of the service, and protection to a consumer against unilateral changes in tariff;

(vi) Requirement on operator(s) to establish and maintain robust complain handling and resolution mechanisms; and

(vii) Operator required to maintain confidentiality of consumer's data/information.

13. What legal protections are offered in relation to the creators of computer software?

Pursuant to the Copyright Ordinance 1962 (the "**Copyright Ordinance**"), any person who knowingly infringes or abets the infringement of:

a) the copyright in a work, or

b) the rental rights in cinematographic works and computer programmes

c) the rights of performers or producers of sound recording; or

d) any other right conferred by this Copyright Ordinance

shall be punishable with imprisonment which may extend to three years, or with fine which may extend to one hundred thousand rupees", or with both.

14. Do you recognise specific intellectual property rights in respect of data/databases?

For the purpose of the Copyright Ordinance, the entitlement to copyright in compilation of data or other material shall not extend to data or other material itself, and shall be without prejudice to any copyright subsisting the data or other material, that is to say, the copyright shall subsist to the extent of the compilation only.

15. What key protections exist for personal data?

The unauthorized access, unauthorized copying, transmission of data or information system with the intent of injury, wrongful gain, wrongful loss or harm to any person shall be treated as a punishable offence. The Federal Government or PTA, as the case may be, may issue directives to be followed by the owners of the designated information systems or service providers in the interest of preventing any offence under applicable law. Whoever obtains, sells, possesses, transmits or uses another person's identity information without authorization is a punishable offence.

Further, all licensees of PTA are required to take all reasonable steps to ensure that those of its employees who obtain, in the course of their employment, information about customers of the licensee or about the customer's business ("Customer Information"), observe the provisions of a code of practice on the confidentiality of Customer Information (the "Confidentiality Code"). Such Confidentiality Code is required to be prepared by the licensee in consultation with PTA and shall, (a) specify the persons with whom Customer Information may not be disclosed to without the prior consent of that customer; and (b) regulate the Customer Information which may be disclosed without prior consent of that customer.

Additionally, all licensees of PTA are required to maintain confidentiality of information about consumers and also require each licensee to ensure that no information about consumers' use of network or service is made available to any third person other than what is printed and published in services directories, agreed by the consumer or required by applicable law. We note from experience that a license granted to a licensee of PTA in Pakistan, generally inter alia contains a provision; that information about customers may only be disclosed to a third-party if the following conditions are complied with; (a) nature of the information to be disclosed has been specified; (b) recipient of the information is disclosed; (c) purpose of the disclosure has been provided; and (d) the customer has provided consent to such disclosure.

A draft data protection bill is in the process of being promulgated, which provides for certain additional protections to all data subjects, in terms of a data controller processing personal information of such data subjects. Pursuant to the law, the definition of the term "personal data" has been widened to include inter alia any information that related directly or indirectly to a data subject whereby, a data controller shall (when once the law is promulgated) be required to provide to the data subject in written notice, the legal basis for the processing of personal data and time duration for which the data is likely to be processed and retained thereafter.

The standards to protect personal data from any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction shall be prescribed by the National Commission for Personal Data Protection (the "NCPDP"), a body envisaged to be incorporated under the new data protection legislation. However, since the law has not yet been promulgated, the requirements thereunder are not yet applicable.

16. Are there restrictions on the transfer of personal data overseas?

Subject to our responses to item 9 above, the restriction in terms of transfer of data overseas currently only applies to licensees of PTA, where such a licensee is required to take reasonable measures to prevent information about its subscribers, from being disclosed to third parties, including the licensee's own subsidiaries, affiliates and associated companies.

Additionally, there is a draft data protection legislation which is in the process of being promulgated; once it is promulgated, it will impose obligations on data controllers to the effect that that personal data shall not be allowed to be transferred to any unauthorized person or system; provided that if personal data is required to be transferred to any system located beyond territories of Pakistan or system that is not under the direct control of any of the governments in Pakistan, it shall be ensured that the country where the data is being transferred offers personal data protection equivalent to the protection provided under the Pakistani legislation, and the data so transferred shall be processed in accordance with the data protection legislation and, where applicable, the consent given by the data subject. However, since the law has not yet been promulgated, the requirements thereunder are not yet applicable.

17. What is the maximum fine that can be applied for breach of data protection laws?

With respect to data protection/privacy, while requirements exist for licensees of PTA to maintain general privacy and confidentiality of the data of their subscribers, under the respective terms of such licensee's license and PTA Laws, there are no specific laws which regulate 'data protection' in Pakistan, and while PECA criminalizes unlawful or unauthorized access to information, data, copying or transmission of critical infrastructure data, it does not regulate 'data protection' in Pakistan.

Having stated the foregoing, in the event that PTA determines that a licensee has violated a provision of this license, PTA Laws, the conditions of its license, any other order or instructions of PTA, PTA may by order impose one or more sanctions provided in the relevant PTA Laws.

Under the applicable PTA Laws, an operator can be subject to a maximum fine of PKR 350 Million (approx. US\$ 2,350,000) or in case of a grave or persistent contravention of its license, PTA may even proceed to terminate the license of the licensee, subject to certain conditions.

The following is the maximum liability in the event of breach of data privacy under PECA:

(i) unauthorized access to information system or data - imprisonment for up to three months or with fine which may extend to fifty thousand rupees or with both;

(ii) unauthorized copying or transmission of data - imprisonment for up to six months, or with fine which may extend to one hundred thousand rupees or with both;

(iii) interference with information system or data - imprisonment for up to two years or with fine which may extend to five hundred thousand rupees or with both;

(iv) unauthorized access to critical infrastructure information system or data - imprisonment for up to three years or with fine which may extend to one million rupees or with both;

(v) unauthorized copying or transmission of critical infrastructure data - imprisonment for up to five years, or with fine which may extend to five million rupees or with both;

(vi) interference with critical infrastructure information system or data - imprisonment for up to seven years or with fine which may extend to ten million rupees or with both;

(vii) unauthorized use of identity information - imprisonment for up to three years or with fine which may extend to five million rupees, or with both; and

(viii) unauthorized interception - imprisonment for up to two years or with fine which may extend to five hundred thousand rupees or with both.

18. What additional protections have been implemented, over and above the GDPR requirements?

With reference to our response to item 11 above, there are no specific laws which regulate 'data protection' in Pakistan, and while PECA criminalizes unlawful or unauthorized access to information or data, copying or transmission of critical infrastructure data, it too does not regulate 'data protection' in Pakistan.

The MOITT has tried to capture and reflect the broad concepts of enhanced protections against unnecessary data collection, and use of data in unanticipated ways, as provided for in the GDPR, however, the draft Pakistan Data Protection Draft Bill is still in the process of being promulgated, and is therefore subject to changes by the legislators.

19. Are there any regulatory guidelines or legal restrictions applicable to cloud-based services?

No.

20. Are there specific requirements for the validity of an electronic signature?

The primary legislation relating to electronic and digital signatures in Pakistan, is the

Electronic Transactions Ordinance 2002 (the “**ETO**”). The relevant applicable laws in this regard are technology neutral.

ETO *inter alia* provides that, the requirement under any law for affixation of signatures shall be deemed satisfied where electronic signatures or advanced electronic signature are applied. An electronic signature may be proved in any manner, in order to verify that the electronic document is of the person that has executed it with the intention and for the purpose of verifying its authenticity or integrity or both. In any proceedings, involving an advanced electronic signature, it shall be presumed unless evidence to contrary is adduced, that:

- a) the electronic document is affixed with an advanced electronic signature, as is the subject-matter of or identified in a valid accreditation certificate is authentic and has integrity; or
- b) the advanced electronic signature is the signature of the person to whom it correlates, the advanced electronic signature was affixed by that person with the intention of signing or approving the electronic document and the electronic document has not been altered since that point in time

The term “electronic signature” has been defined in the ETO as “any letters, numbers, symbols, images, characters or any combination thereof in electronic form, applied to, incorporated in or associated with an electronic document, with the intention of authenticating or approving the same, in order to establish authenticity or integrity, or both”.

The term ‘advanced electronic signature’ has been defined in the ETO as “an electronic signature which is either:

- (i) unique to the person signing it, capable of identifying such person, created in a manner or using a means under the sole control of the person using it, and attached to the electronic document to which it relates in a manner that any subsequent change in the electronic document is detectable; or
- (ii) provided by an accredited certification service provider and accredited by the Certification Council as being capable of establishing authenticity and integrity of an electronic document”.

The applicable laws in Pakistan do not provide for any specific transactions that require one type of electronic signature over another. However, it provides that a government entity/body may accept *inter alia* the filing of documents, or creation or retention of such documents in the form of electronic documents, and issue permits, certificate, license or approval in the form of electronic document(s).

In instances where the government entity/body decides to undertake any of the foregoing, it may specify:

- a) the manner and format in which such electronic documents shall be filed, created, retained or issued;
- b) when such electronic document(s) has to be signed, the type of electronic signature, advanced electronic signature or a security procedure required;
- c) the manner and format in which such signature shall be affixed to the electronic document, and the identity of or criteria that shall be met by any certification service provider used by the person filing the document;
- d) control process and procedures as appropriate to ensure adequate integrity, security and confidentiality of electronic documents, procurement, transactions or payments; and
- e) any other required attributes for electronic documents or payments that are currently specified for corresponding paper documents.

With regards to evidentiary value of the electronic or advanced electronic signature, please note that both electronic and advanced electronic signatures are legally recognized in Pakistan and bear the same evidentiary value in the court of law.

Where an electronic document is alleged to be signed or to have been generated wholly or in part by any person through the use of an information system, and where such allegation is denied, the application of a security procedure to the signature or the electronic document must be proved.

It may be noted that however, certain types of transactions are specifically prohibited from the use of electronic signatures. The provisions of ETO shall not apply to the following:

- (i) a negotiable instrument (a promissory note, bill of exchange or cheque payable either, to order or to bearer) as defined under the Negotiable Instruments Act, 1881;
- (ii) a power-of-attorney under the Powers of Attorney Act, 1881;
- (iii) a trust (an obligation annexed to the ownership of property, and rising out of a confidence reposed in and accepted by the owner, or declared and accepted by him, for the benefit of another, or of another and the owner) as defined under the Trust Act 1882, but excluding constructive, implied and resulting trusts;

(iv) a will or any form of testamentary disposition under any law for the time being in force; and

(v) a contract for sale or conveyance of immovable property or any interest in such property.

21. In the event of an outsourcing of IT services, would any employees, assets or third party contracts transfer automatically to the outsourcing supplier?

The law does not provide for an automatic transfer of employees, assets or third-party contracts in case of an outsourcing arrangement. The transfers, if any, will only be guided by the contractual terms agreed to between the parties.

22. If a software program which purports to be a form of A.I. malfunctions, who is liable?

There is no specific legislation in Pakistan to regulate A.I. and courts in Pakistan are yet to adjudicate on a matter involving loss/ harm caused due to an A.I. based system. In the current scenario, any system or product based on A.I. will have to be treated at par with a similar system or product not based on A.I., and remedies available to consumers vis-à-vis such system or product based on A.I. will be the same as otherwise available to such person.

An affected person may seek remedy under the applicable consumer protection laws, or in the event of damage incurred by such party, the same may be recoverable to the extent that the actual damage incurred can be proved.

23. What key laws exist in terms of: (a) obligations as to the maintenance of cybersecurity; (b) and the criminality of hacking/DDOS attacks?

a) obligations as to the maintenance of cybersecurity; and

While there are no general obligations in the applicable law vis-à-vis maintenance of cybersecurity, PECA criminalizes any unauthorized access to information system, unauthorized copying of any data, access to any critical infrastructure, electronic fraud, tampering with communication information, offences against person modesty or decency, writing malicious codes or their transmission, cyber stalking, hate speech or glorification of an offence.

PECA provides for the constitution of a Computer Emergency Response Teams (CERT), to respond to any threat against or attack on any critical infrastructure information systems or critical infrastructure data, or widespread attack on information systems in Pakistan. In order to achieve this, PTA has prepared an implementation framework titled "CERT (Computer Emergency Response Team) - Pakistan Telecom Sector Implementation Plan". The framework is pertinent to the country's telecom sector and recommends steps to be taken by

PTA in order to establish such teams. The framework delineates upon functions and roles of the CERT.

Further, sectoral regulators, such as the State Bank of Pakistan (SBP) and Securities and Exchange Commission of Pakistan (SECP) prescribe cybersecurity measures to be adhered to by the players within their respective domains. For example, SBP requires financial institutions to develop, document, implement and regularly review a formal comprehensive IT security framework and policy for their branch-less banking systems.

Additionally, a National Response Centre for Cyber Crime (NR3C) has been established by the Federal Investigation Agency (FIA) to identify and curb the phenomenon of technological abuse in society, and to deal with technology-based crimes in Pakistan.

b) the criminality of hacking/DDOS attacks?

The Information Technology Act, 2000 (IT Act) contains sufficient provisions to criminalize both hacking and DDOS attacks; shall be punishable with imprisonment, under the, are prohibited, when committed in the absence of consent from the owner or person in charge of such computer, computer system or computer network. Providing assistance to any person involved in any of the above listed activities is also treated at par with the actual act committed. The nature and intent of hacking/ conduct of DDOS attacks may also trigger provisions under the Indian Penal Code, 1860.

PECA contains provisions to criminalize both hacking and DDOS attacks. Though these terms are not defined under PECA, activities such as gaining unauthorized access to any information system or data, copying or otherwise transmitting or causing to be transmitted any data, or interfering with or damaging or causing to be interfered with or damaging any part or whole of an information system or data, or interfering with or damaging, or causing to be interfered with or damaged, any part or whole of a critical information system, or data are prohibited and punishable, when committed in the absence of consent from the owner or person in charge of such information system or data.

Additionally, depending on the nature and intent of hacking/ conduct of DDOS attack(s), relevant provisions under the Pakistan Penal Code 1860 may also be triggered.

24. What technology development will create the most legal change in your jurisdiction?

Technologies such as artificial intelligence, machine learning, robotics, 3D printing, blockchain, the internet of things, and neurotechnology are cutting-edge technologies that had limited practical applications until some time back, but have come to pervade daily life in a short span of time, and are galvanizing a paradigm shift in technological advances.

Having stated the foregoing, the front runners for technology which is potentially likely to create the most legal change in Pakistan is A.I and blockchain technology.

In recent news, a leading microfinance banks in Pakistan, in partnership with a Malaysian entity, has introduced Pakistan's first blockchain-based cross-border remittance service, powered by industry-leading blockchain technology.

While SBP has prohibited banks and financial institutions regulated by it, from dealing with cryptocurrencies, the Government acknowledges the potential of blockchain technology. Currently, there is no regulatory framework in place to govern the use of such technology and related services in Pakistan.

25. Which current legal provision/regime creates the greatest impediment to economic development/ commerce?

The draft data protection legislation for Pakistan proposes to introduce data localization requirements. The same has the potential of being anti-commerce and may have the potential to slow economic growth. Having said the same, since the law has not yet been promulgated, the requirements thereunder are not yet applicable.

In terms of legal gaps which exist, if removed, could improve the pace of economic development/commerce with a specific focus on the technology regime, would be the introduction of legal framework(s) for developing technology (including technologies such as blockchain) so that the economy can benefit from the same.

26. Do you believe your legal system specifically encourages or hinders digital services?

The Pakistani legal system creates a conducive environment for the growth of digital services in Pakistan, as a large majority of digital services continue to be provided without many conditions or restrictions. However, the communication network/ infrastructure that facilitates digital services is tightly regulated.

27. To what extent is your legal system ready to deal with the legal issues associated with artificial intelligence?

While policy framers do recognise A.I. as one of the likely causes for the next stage of technological evolution of the digital economy, the same is not regulated by any legislation. A system or product utilizing A.I. technology is presently treated at par with any other system or product of similar nature.