Legal 500
Country Comparative Guides 2025

Pakistan
TMT

Contributor

Chima & Ibrahim

Aneeq Shah

Associate | aneeq.shah@chima-ibrahim.com

Yasser Hamdani

Senior Counsel | yasser.hamdani@chima-ibrahim.com

Ali Asim

Partner | ali.asim@chima-ibrahim.com

Shazil Ibrahim

Partner | shazil.ibrahim@chima-ibrahim.com

This country-specific Q&A provides an overview of tmt laws and regulations applicable in Pakistan.

For a full list of jurisdictional Q&As visit **legal500.com/guides**

Pakistan: TMT

1. Software – How are proprietary rights in software and associated materials protected?

Proprietary rights in software are primarily protected under Pakistan's copyright laws. The definition of 'literary works' in the Copyright Ordinance, 1962 ("Copyright Ordinance") includes 'compilations and computer programmes, that is to say programmes recorded on any disc, tape, perforated media or other information storage device, which, if fed into or located in a computer or computer-based equipment is capable of reproducing any information'. While registration is not required, it is advisable and can serve as prima facie evidence in case of infringement which makes it easier to enforce rights. The Copyright Ordinance grants the author exclusive rights to reproduce, modify and distribute the software. Associated materials such as software manuals, documentation etc. are also protected as literary works. The rights are enforceable through civil remedies for infringement (injunction and damages) and also through criminal prosecution resulting in fines and imprisonment. Software is not subject to patent protection under Pakistan's Patent Ordinance, 2000 though it may be possible to patent a process which includes a novel software and hardware combination. Software licensing and user agreements are enforceable under the law, allowing parties to define rights and obligations over software use. Although Pakistan does not have a standalone trade secrets law, confidential information is protected through non-disclosure agreements and confidentiality undertakings, and through common law torts such as breach of confidence.

2. Software – In the event that software is developed by a software developer, consultant or other party for a customer, who will own the resulting proprietary rights in the newly created software in the absence of any agreed contractual position?

In the absence of an agreed contractual provision, the general rule under Pakistani copyright law is that the author (i.e., the person who creates the software) is the first owner of the copyright.

- However, if the software is created by an employee in the course of employment, the employer is typically considered the owner of the copyright, unless otherwise agreed.
- For consultants, freelancers, or third-party developers, the developer retains ownership of the copyright, and the customer only receives a license to use the software. Therefore, explicit contractual arrangements are crucial to transfer ownership to the customer though the customer will likely have an implied license to use the software for the purpose it was developed.
- This position aligns with common law principles, and Pakistani courts are likely to follow similar reasoning.

3. Software – Are there any specific laws that govern the harm / liability caused by Software / computer systems?

The general principles of contract law, tort law (such as negligence), and consumer protection laws would apply if software causes harm or financial loss. Also, the Prevention of Electronic Crimes Act, 2016 ("PECA") has been enacted to prevent unauthorised acts with respect to information systems and provides for offences, such as wilfully and without authorisation writing, offering, making available, distributing or transmitting malicious code through an information system or device, with intent to cause harm to any information system or data resulting in the corruption, destruction, alteration, suppression, theft or loss of the information system or data. Thus, PECA is relevant in cases involving malicious software or unauthorised access, though it is focused more on criminal liability than civil damages.

4. Software – To the extent not covered by (3) above, are there any specific laws that govern the use (or misuse) of software / computer systems?

Other offences under PECA include unauthorised access to information system or data; unauthorised copying or transmission of data; interference with critical information system or data; unauthorised copying or transmission of critical infrastructure data; glorification of an offence; cyber terrorism; hate speech; recruitment, funding and planning of terrorism; electronic forgery and fraud; unauthorised use of identity information; unauthorised issuance of SIM cards; offences against modesty or dignity of a natural person or minor; child pornography; solicitation and cyber enticement;

commercial sexual exploitation of children; use of information system for kidnapping, abduction or trafficking of a minor; cyber stalking; cyberbullying; disseminating, exhibiting or transmitting false and fake information; spamming and spoofing.

The telecom laws and regulations may also apply in certain cases.

Unauthorised alteration, modification, deletion, removal, generation, transmission or storage of information (which includes text, message, data, voice, sound, database, video signals, software, computer programs, codes including object code and source code) is an offence under the Electronic Transactions Ordinance, 2002 ("ETO"). Unauthorised impairment to the operation of, or prevention or hindering access to any information contained in any information system (i.e., an electronic system for creating, generating, sending, receiving, storing, reproducing, displaying, recording or processing information) is also an offence under ETO. Additionally, unauthorised access to information contained in an information system is also an offence under ETO. Certain offences, including but not limited to forgery under the Pakistan Penal Code, 1860 may also be applicable.

5. Software Transactions (Licence and SaaS) – Other than as identified elsewhere in this overview, are there any technology-specific laws that govern the provision of software between a software vendor and customer, including any laws that govern the use of cloud technology?

The Pakistan Ministry of Information Technology & Telecommunication ("MOITT") has introduced policies that impact cloud technology service providers in Pakistan. As an example, the Pakistan Cloud First Policy is applicable to all federal Public Sector Entities (including ministries, departments, and state-owned enterprises) that are required to prioritise cloud-based solutions for new ICT investments. The policy is intended to encourage private sector adoption as well (which is not mandatory). A Cloud Office has been set up which has a key role in implementation of the Policy. Accreditation criteria for cloud service providers to provide services to public service entities have been specified and some cloud service providers have been accredited.

While not technology specific, there are consumer protection laws that address, inter alia, disclosures for products and services and liabilities for defective products and services (which will include software).

Pakistan does not yet have a comprehensive data protection law, but a Bill titled the Personal Data Protection Act, 2023 ("Data Protection Bill") has been under discussion for several years. When enacted, it will significantly impact SaaS and cloud offerings, by introducing consent and purpose limitations, cross-border data transfers and security obligations on processors and controllers.

6. Software Transactions (License and SaaS) – Is it typical for a software vendor to cap its maximum financial liability to a customer in a software transaction? If 'yes', what would be considered a market standard level of cap?

Yes, it is standard practice for software vendors—both for traditional software licenses and SaaS agreements—to cap their maximum financial liability to customers in software transactions. This cap is typically included in the contract as a 'limitation of liability' clause to manage risk and protect vendors from potentially large, unpredictable claims. The most common market standard for liability caps is an amount equal to the fees paid by the customer over a defined period, most often 12 months. In some cases, especially for higher-risk scenarios (such as breaches of confidentiality or data protection), the cap may be increased to up to 3–5 times the annual contract value. Unlimited liability is rarely accepted, but exceptions are typically made for certain breaches, such as fraud, wilful misconduct, breach of confidentiality, or infringement of third-party intellectual property rights. Such caps are generally enforceable under the contract law, provided they are not unconscionable or contrary to public policy. Sophisticated customers (banks, telcos, regulators) often negotiate higher or specific liability limits, especially for mission-critical software.

Consumer protection laws also contain certain limitations. For example, in Punjab, where the only loss due to use of goods or services is a lack of utility/benefit, a vendor will only be liable for a return of the consideration or a part thereof and the costs.

7. Software Transactions (License and SaaS) – Please comment on whether any of the following areas of liability would typically be excluded from any financial cap on the software vendor's liability to the customer or subject to a separate enhanced cap in a negotiated software

transaction (i.e. unlimited liability): (a) confidentiality breaches; (b) data protection breaches; (c) data security breaches (including loss of data); (d) IPR infringement claims; (e) breaches of applicable law; (f) regulatory fines; (g) wilful or deliberate breaches.

It is not uncommon for the financial cap to be subject to specific exceptions.

(a) Confidentiality Breaches

Liability for breaches of confidentiality is commonly excluded from liability caps or it may be included subject to a higher cap. Vendors may accept that because of the sensitive nature of the information and the reputational and legal risks involved.

(b) Data Protection Breaches

Data protection breaches, especially involving personal or sensitive data, are increasingly treated as a separate category with uncapped or significantly enhanced liability caps. Customers push for this due to the high financial and regulatory risks associated with data privacy violations.

Indemnification clauses covering costs related to data breaches (legal fees, notification, credit monitoring, regulatory fines) are common and often uncapped or subject to a higher cap.

(c) Data Security Breaches (Including Loss of Data)

Liability for data security failures, including loss or corruption of data, is at times excluded from caps or subject to enhanced caps, especially where the vendor is responsible for security controls.

In cloud or SaaS agreements, liability may be limited by the shared responsibility model, but where the vendor's negligence causes the breach, uncapped or higher liability is likely to be negotiated.

(d) Intellectual Property Rights ("IPR") Infringement Claims

IPR infringement claims are typically excluded from financial caps or have a separate indemnity with unlimited or higher caps. Vendors usually provide indemnities to protect customers against third-party IP claims.

(e) Breaches of Applicable Law

Liability for breaches of applicable laws, especially those related to data protection, consumer protection, or cybersecurity, is often excluded from caps or is subject to enhanced caps. This ensures vendors remain fully accountable for compliance failures.

(f) Regulatory Fines

Regulatory fines imposed on the customer due to the vendor's actions, especially under data protection or cybersecurity laws, are usually excluded from caps or may be subject to separate indemnification clauses.

Given the increasing size of regulatory penalties globally, customers insist on uncapped liability or indemnification for such fines.

(g) Wilful or Deliberate Breaches

Liability arising from wilful misconduct, deliberate breaches, fraud, or gross negligence is usually excluded from limitation of liability caps.

8. Software Transactions (License and SaaS) – Is it normal practice for software source codes to be held in escrow for the benefit of the software licensee? If so, who are the typical escrow providers used? Is an equivalent service offered for cloud-based software?

There is no Pakistani legal precedent, regulation, or industry guideline mandating or establishing source code escrow as a standard practice in software licensing. Most agreements are negotiated on a case-by-case basis, and escrow is more common in large or sensitive deals, mirroring international trends rather than a Pakistani standard.

9. Software Transactions (License and SaaS) – Are there any export controls that apply to software transactions?

- Pakistan has a stated policy to facilitate software and IT services exports. This can be seen in MOITT's Digital Pakistan Policy where the stated objective to increase software exports and IT remittances as well as to expand the domestic market and in the Strategic Trade Policy Framework 2020-2025 where software export sector is one of the 18 priority sectors identified by the Government of Pakistan for diversifying the export base and strengthening local production. Pursuant to the latter, the Software Development Export Strategy 2023-27 endorsed by

the Ministry of Commerce has been prepared with a five-year plan of action for development of software exports from Pakistan.
- Registering with the Pakistan Software Export Board will, among other things, allow companies exporting IT & IT enabled services to benefit from additional tax incentives for a certain time-period.
- The State Bank of Pakistan ("SBP") regulates foreign exchange aspects of software exports, requiring documentation such as software export agreements or invoices and monitoring remittances related to software exports. The Foreign Exchange Manual of SBP stipulates certain procedures to be followed for the export of computer software and realisation of the proceeds of such exports.
- There are certain restrictions on the export of technologies related to nuclear and biological weapons and their delivery systems under the Export Control on Goods, Technologies, Material and Equipment related to Nuclear and Biological Weapons and their Delivery Systems Act, 2004 commonly referred to as the Export Control Act, 2004. This is administered by the Strategic Export Control Division ("SECDIV") and requires authorisation for the export or transmission of controlled goods, technologies, and software (if it meets specific criteria related to strategic or sensitive use), including through electronic means such as cloud computing. Thus:
    - Exporters must obtain licenses and register with SECDIV for controlled items.
    - Transmission of software or technology outside Pakistan, including by electronic transmission or making it available electronically, is subject to export authorisation.
    - SECDIV can reject applications based on national security, foreign policy, counterterrorism, or non-compliance.

10. IT Outsourcing – Other than as identified elsewhere in this questionnaire, are there any specific technology laws that govern IT outsourcing transactions?

Government incentives and policies support the growth of IT outsourcing but do not create a specific legal regime for IT outsourcing transactions, which thus are regulated through a combination of general laws, including contract law, intellectual property rights, labour laws, tax laws, export controls, foreign exchange regulations, etc.

Where individuals are hired directly by an international firm, Pakistan employment and tax laws will become applicable. Regarding employment laws, if an individual is hired as a freelancer or independent contractor then these may not apply, however, there is a risk that the freelancer or independent contractor may be classified as an employee under Pakistani law (if the nature of work is similar to that of an employee and the international company retains control over his work as an employer would).

11. IT Outsourcing – Please summarise the principal laws (present or impending), if any, that protect individual staff in the event that the service they perform is transferred to a third party IT outsource provider, including a brief explanation of the general purpose of those laws.

Under Pakistan law, if an employee is to be transferred to a third party (i.e., they would then become the employee of the third party), this would effectively constitute termination of the existing employment and re-hiring by the new employer and would naturally require the consent of the employee. Any end of service benefits would need to be paid out or absorbed (under agreement with the employee) by the third party.

If services are merely to be seconded to the third party (for a limited period of time or project), the employee would continue to be the employee of the original employer, who would be liable to the employee in respect of the statutory or contractual benefits to be paid to the employee.

There is also a practice in Pakistan to outsource certain services, and not to treat the persons who are providing such services as employees of the company (but to present them as employees of the third-party contractor). A recent judgment of the Supreme Court of Pakistan in ***IFFCO Pakistan v. Ghulam Murtaza (2024 SCMR 1548)*** is the authoritative precedent emphasising that genuine outsourcing is lawful, but this must not be used to evade workers' rights. The degree of employer control is thus key to determining employee status and entitlements. Continuity of employment and social security protections apply, and sham outsourcing arrangements are prohibited.

There are also provincial employment laws to protect employees providing 'skilled or unskilled, manual or clerical' work, but these do not generally apply to employees in the management cadre, and the terms of employment of the latter are mostly governed by contract.

12. Telecommunications – Please summarise the principal laws (present or impending), if any, that govern telecommunications networks and/or services, including a brief explanation of the general purpose of those laws.

The principal legislation that deals with telecommunication networks and/or services is the Pakistan Telecommunication (Re-Organization) Act, 1996 ("Telecom Act") and the rules and regulations made under it. The Telecom Act inter alia, establishes the Pakistan Telecommunication Authority ("PTA") and the Frequency Allocation Board. The Telecom Act also governs the regulation of the telecommunication industry, the privatisation of telecommunication services, and related matters.

In some regions which are not constitutionally part of Pakistan, the Telecom Act was adopted through separate procedure. In Azad Jammu and Kashmir, the Telecom Act was adopted through the Azad Jammu and Kashmir Council Adaption of Pakistan Telecommunication (Re-Organization) Act, 2005. In Gilgit Baltistan it was adopted through the Northern Areas Telecommunication (Re-organization) (Adaption and Enforcement) Order, 2006 followed by the Gilgit-Baltistan Council Adaptation of Laws Act, 2012 and its amendment in 2014.

PTA regulates the establishment, operation and maintenance of telecommunication systems and the provision of telecommunication services in Pakistan and has issued detailed regulations covering technical standards, licensing conditions, and equipment approval to ensure network security, reliability, and consumer protection by enforcing quality and safety standards on telecom infrastructure and devices. The Frequency Allocation Board allocates and assigns portions of the radio frequency spectrum to Government, providers of telecommunication services and telecommunication systems, radio and television broadcasting operations, public and private wireless operators and others.

PECA also applies as it requires telecom service providers to retain traffic data for a specified time-period. It also criminalises unauthorised access, hacking, and data breaches affecting telecom networks.

Some legacy laws such as The Wireless Telegraphy Act, 1933 and the Telegraph Act, 1885 while still in the field have been largely supplanted in practice by the provisions of the Telecom Act.

The Digital Nation Pakistan Act, 2025 is a recent law which aims to transform Pakistan into a digital economy. It establishes the National Digital Commission and the Pakistan Digital Authority to coordinate digital governance, policy, and infrastructure development nationwide. It aims to foster a secure, inclusive, and interoperable digital ecosystem supporting innovation, connectivity, and efficient public service delivery, which includes telecommunications as a critical infrastructure.

The relevant consumer protection laws provide for protection and promotion of the rights and interests of consumers which include telecom consumers.

13. Telecommunications – Please summarise any licensing or authorisation requirements applicable to the provision or receipt of telecommunications services in your country. Please include a brief overview of the relevant licensing or authorisation regime in your response.

The Telecom Act stipulates that every person is required to have license to establish, maintain or operate any telecommunication system or provide any telecommunication service. Telecommunication system has been defined to include any electrical, electromagnetic, 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 re-arrangement, 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. Telecommunication service has been defined to include 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 re-arrangement, computation or any other process in the course of the service.

Provision of telecommunications services or operating a telecommunication system in Pakistan (excluding provision of terrestrial wireless radio broadcasting and Television broadcasting within Pakistan and some other exceptions such as but not limited to provision of telecom services or operating a telecom system by the police or security services) thus require appropriate licenses from PTA tailored to the service type. The licensing framework is comprehensive, covering traditional telecom services such as fixed line, long distance and mobile services, satellite communications, mobile virtual network operators, infrastructure providers,

internet service providers, value added services and emerging data services like VPNs. Licensees must comply with strict regulatory conditions related to national security, lawful interception, data protection, and service quality. PTA's licensing process involves application review, security vetting, and adherence to ongoing compliance obligations. Operators in Pakistan must obtain licenses from PTA tailored to their operational model and in relation to some value-added services register with PTA.

Mobile network operators ("MNOs") hold full infrastructure licenses and spectrum rights, whereas Mobile Virtual Network Operators may operate via agreements with MNOs under a new, more accessible licensing framework aimed at increasing competition and service diversity. Other telecom-related services such as satellite communications, VPNs, and value-added internet services are regulated through specific licensing or registration regimes. This licensing framework ensures regulatory oversight, service quality, national security compliance, and consumer protection in Pakistan's telecommunications sector.

A license is thus required, inter alia, to operate as cellular mobile operator, establish and operate electronic information services, to provide local loop/VAS/long distance/infrastructure services etc.

14. Telecommunications – Please summarise the principal laws (present or impending) that govern access to communications data by law enforcement agencies, government bodies, and related organisations. In your response, please outline the scope of these laws, including the types of data that can typically be requested, how these laws are applied in practice (e.g., whether requests are confidential, subject to challenge, etc.), and any legal or procedural safeguards that apply.

Pakistan's legal regime allows law enforcement and government bodies significant powers to access communications data, primarily under PECA, as supplemented by PTA's regulatory authority.

The Telecom Act allows the Federal Government of Pakistan to authorise any person or persons to intercept call and messages or to trace calls through any telecommunication systems in the interest of national security or in the apprehension of any offence. Telecom operators are required to assist in the lawful interception of data under the Telecom Act.

PECA requires telecom service providers to retain traffic data for a minimum of one year or such period as PTA may notify. PECA also empowers the authorised officer to apply for a warrant for search and seizure of an information system, data, device or other articles from the relevant court. It also allows for an application of a warrant to access content data stored in an information system. Both of these warrants are for the purposes of a criminal investigation or criminal proceedings. There is no formal process to challenge these orders but judicial oversight is built into the process.

PECA also provides for the real-time collection and recording of information including communications for the purposes of a criminal investigation, after receiving the relevant court's approval. There is no formal process to challenge these orders however, judicial oversight is built into the process.

The Investigation for Fair Trial Act, 2013 ("IFTA") provides the relevant court the authority to pass a warrant for surveillance or interception of communications of a person associated with or beginning to get associated with any act leading to an offence provided in the schedule of IFTA. There is no formal process to challenge these orders however, judicial oversight is built into the process.

Lastly, there is the Data Protection Bill which has been under consideration for a number of years. It is meant to regulate the collection, processing and disclosure of personal data. It is not clear what impact it could have on the collection of data by law enforcement agencies.

15. Mobile communications and connected technologies – What are the principle standard setting organisations (SSOs) governing the development of technical standards in relation to mobile communications and newer connected technologies such as digital health or connected and autonomous vehicles?

PTA is the primary mobile communications and connected technologies regulator in Pakistan. It regulates the establishment, operation and maintenance of telecommunication systems in Pakistan, and also has the function to promote rapid modernisation of telecommunication systems and telecommunication services. PTA requires compliance with internationally recognised SSOs such as ITU-T, ETSI, ISO, FCC, CENELEC, and IEC through the Type Approval Standards

Regulations, 2018. These bodies govern technical standards for mobile communications (including 4G/5G), digital health, connected vehicles, and other emerging connected technologies. PTA's regulations ensure that devices and networks deployed in Pakistan meet global interoperability, safety, and security benchmarks.

MOITT is responsible for the preparation of an overall integrated plan as well as formulation of policy for the development and improvement of information technology and telecommunications, including related infrastructure, in Pakistan.

16. Mobile communications and connected technologies – How do technical standards facilitating interoperability between connected devices impact the development of connected technologies?

Technical standards facilitating interoperability between connected devices play a crucial role in the development of connected technologies in Pakistan's mobile communications landscape. Telecommunication operators are required to ensure interconnection between telecommunication systems upon request by other telecommunication operators. The telecommunication operators are required to comply with all relevant international standards, including, without limitation, those of the International Telecommunication Union This is an area regulated by PTA.

17. Data Protection – Please summarise the principal laws (present or impending), if any, that that govern data protection, including a brief explanation of the general purpose of those laws.

Pakistan currently does not have a comprehensive data protection law. The Data Protection Bill has been in discussion for a number of years but it has not been enacted. There have been indications that Pakistan has been recently working on finalising the Data Protection Bill and it may be enacted into law soon. The aim of the draft law is to provide protection with regard to the processing of electronic data in Pakistan, while also respecting the rights, freedom and dignity of natural and legal persons (with special regard to their right to privacy, secrecy and personal identity and matters connected therewith). It is noted that after its enactment there will be an advance notice period before it is implemented.

The right to privacy (including privacy of information) is protected in the chapter on fundamental rights in the Constitution of the Islamic Republic of Pakistan, 1973. It is also recognised by certain laws and elucidated by decisions of the superior courts of Pakistan. The relevant laws, among others, that recognise the right to privacy, and which make unauthorised disclosure or use of personal information punishable, include:

- Constitution of the Islamic Republic of Pakistan, 1973
- Banking Companies Ordinance, 1962
- Pakistan Telecommunications (Re-organization) Act, 1996
- National Database Registration Authority Ordinance, 2000
- Electronic Transactions Ordinance, 2002
- Payment Systems and Electronic Funds Transfers Act, 2007
- Telecom Consumer Protection Regulations, 2009
- Prevention of Electronic Crimes Act, 2016
- Right of Access to Information Act, 2017
- Protection of Journalists and Media Professional Act, 2021
- Protection Against Harassment of Women at the Workplace Act, 2010

The scheme of the Pakistani Constitution and certain observations of the Supreme Court of suggest that if privacy rights were to be violated by a private person, even outside the scope of those laws, recourse to courts may be available (e.g., by way of injunction or damages). Moreover, certain laws, such as PECA, prescribe punishment for the breach of privacy.

18. Data Protection – What is the maximum sanction that can be imposed by a regulator in the event of a breach of any applicable data protection laws?

The courts may award injunction or damages that depend on the circumstances of the case. Under PECA the maximum potential punishment is a 7-year prison sentence and/or a fine which may extend to PKR 10,000,000/-. Under the proposed Data Protection Bill, the maximum fine that can be levied is USD 2,000,000/-. Notwithstanding this, a legal person can be punished with a fine not exceeding 1% of annual gross revenue in Pakistan or USD 200,000/- whichever is higher.

19. Data Protection – Do technology contracts in your country typically refer to external data protection regimes, e.g. EU GDPR or CCPA, even where the contract has no clear international

element?

It is not the standard practice for purely domestic contracts to incorporate these external data protection regimes. Contracts which involve a foreign party do typically refer to an external data protection regime, such as EU GDPR or CCPA.

20. Cybersecurity – Please summarise the principal laws (present or impending), if any, that that govern cybersecurity (to the extent they differ from those governing data protection), including a brief explanation of the general purpose of those laws.

Pakistan's cybersecurity legal framework is primarily governed by PECA, (as amended most recently by the Prevention of Electronic Crimes (Amendment) Act, 2025) and addresses cybercrime regulation, content control, and enforcement powers. PECA makes it an offence for a person to access an information system or data without authorisation, copy or transmit data without authorisation, interfere with an information system or data, access critical infrastructure information system or data without authorisation, copy or transmit critical infrastructure data without authorisation, or intercept, distribute or transmit malicious code, cyber stalk, cyber bully and spam.

This is complemented by PTA's Cyber Security Strategy 2023-2028 read with the National Cyber Security Policy, 2021. PTA has issued a five-year Cyber Security Strategy aiming to build digital resilience across the telecom sector. Its purpose is to strengthen legal frameworks, promote cyber resilience, improve incident response, and foster public-private partnerships to combat cyber threats.

The Telecom Act also makes it an offence for any person who intercepts or acquaints himself with the contents of any intelligence (i.e., any speech, sound, data, signal, writing, image or video) or without authorisation discloses to any person the contents of such intelligence.

Additionally, ETO makes it an offence for any person to gain unauthorised access to any information system (i.e., an electronic system for creating, generating, sending, receiving, storing, reproducing, displaying, recording or processing information where information includes text, message, data, voice, sound, database, video Signals, software, computer programs, codes including object code and source code).

The Data Protection Bill also has provisions requiring the adoption of adequate data security measures. It also includes the requirement of breach notification and the setting up of accrediting bodies to audit the security measures of data controllers and processors.

21. Cybersecurity – What is the maximum sanction that can be imposed by a regulator in the event of a breach of any applicable cybersecurity laws?

PECA empowers the courts to sanction a range of offences. The following are of note:

a. interfering with or causing damage or loss to critical infrastructure information systems or data i.e., information system or data that supports or performs a function with respect to a critical infrastructure (the loss or compromise of which could have a major detrimental impact on availability of essential services such as those that could result in significant loss of life or casualties, or significant impact on national security, national defence or functioning of the state) – maximum of 7 years imprisonment and/or a fine which may extend to PKR 10,000,000/-
b. unauthorised access to information system/data – maximum of 3 months imprisonment and/or a fine which may extend to PKR 50,000/-
c. unauthorised copying/transmission of data – maximum of 6 months imprisonment and/or fine which may extend to PKR 100,000/-
d. interference with system/data – maximum of 2 years imprisonment and/or fine which may extend to PKR 500,000/-
e. unauthorised access to critical infrastructure – maximum of 3 years imprisonment and/or a fine which may extend to PKR 1,000,000/-
f. unauthorised copying of critical infrastructure data – maximum of 5 years imprisonment and/or a fine which may extend to PKR 5,000,000/-
g. tampering of communication equipment – maximum of 3 years imprisonment and/or a fine which may extend to PKR 1,000,000/-
h. unauthorised interception there is – maximum of 2 years imprisonment and/or a fine which may extend to PKR 500,000/-
i. writing, offering or making available, distributing or transmitting malicious code through an information system or device – maximum of 2 years imprisonment and/or a fine which may extend to PKR 1,000,000/-

In terms of the Telecom Act imprisonment for offence noted above may extend to 3 years, and/or a fine which

may extend to PKR 10,000,000/-.

Under ETO, for violation of privacy noted above and for unauthorised alteration, modification, deletion, removal, generation, transmission or storage pf any information through or in any information system, maximum punishment is 7 years and/or fine which may extend to PKR 1,000,000/-.

Under the proposed Data Protection Bill, the regulator may impose a fine of up to USD 50,000/- on companies for not having adequate security measures. Please also see our responses in Section 18.

22. Artificial Intelligence – Which body(ies), if any, is/are responsible for the regulation of artificial intelligence?

Pakistan currently does not have any legislation related to artificial intelligence. MOITT is working on introducing a National Artificial Intelligence Policy ("NAIP"); however, it is currently in draft form. NAIP envisages the creation of the National Artificial Intelligence Fund and Centres of Excellence. A Bill titled the Regulation of Artificial Intelligence Act, 2024 ("AI Bill") that has been introduced in the Senate proposes to set up the National Artificial Intelligence Commission with the power to engage in legal actions, manage property, and maintain operational autonomy.

23. Artificial Intelligence – Please summarise the principal laws (present or impending), if any, that that govern the deployment and use of artificial intelligence, including a brief explanation of the general purpose of those laws.

Pakistan currently does not have any legislation related to artificial intelligence – the AI Bill is pending in the Senate of Pakistan and MOITT is working on introducing NAIP. The policy aims to provide a national strategy to establish an ecosystem necessary for AI adoption. It stems from the 'AI for good' initiative by the International Telecommunication Union and the Sustainable Development Goals set forth by the United Nations.

24. Artificial Intelligence – Are there any specific legal provisions (present or impending) in respect of the deployment and use of Large Language Models and/or generative AI (including agentic AI)?

There are currently no such legal provisions. If the AI Bill is made into law, a new regulatory body will be created to regulate the deployment and use of Large Language Models and/or generative AI.

25. Artificial Intelligence – Do technology contracts in your jurisdiction typically contain either mandatory (e.g. mandated by statute) or recommended provisions dealing with AI risk? If so, what issues or risks need to be addressed or considered in such provisions?

This has not been a standard practice so far.

26. Artificial Intelligence – Do software or technology contracts in your jurisdiction typically contain provisions regarding the application or treatment of copyright or other intellectual property rights, or the ownership of outputs in the context of the use of AI systems?

This has not been a standard practice so far.

27. Blockchain – What are the principal laws (present or impending), if any, that govern (i) blockchain specifically (if any) and (ii) digital assets, including a brief explanation of the general purpose of those laws?

The government, has been promoting the use of blockchain and cryptocurrency in Pakistan, and has set up a Pakistan Crypto Council ("PCC") which aims to regulate, among other things, blockchain technologies.

On the recommendation of PCC, the Pakistan Digital Assets Authority ("PDAA") was formed in March, 2025 and is to act as the primary regulator once operational. The regulatory approach focuses on consumer protection, compliance with global standards, and fostering innovation to integrate blockchain and digital assets into Pakistan's financial system.

Until recently, crypto trading had been effectively banned by SBP. In May 2025, however, SBP appeared to soften its approach and noted that virtual assets are not illegal per se, but rather that there are no legal and regulatory frameworks relating to them. SBP also noted that they have engaged with PCC to develop an appropriate legal and regulatory framework.

In July 2025 the President of Pakistan enacted the Virtual

Assets Ordinance, 2025 ("VAO") – being an ordinance passed by the President, VAO will expire 120 days from its inception (this can be extended for one additional period of 120 days by either of the two houses of the federal legislature) unless passed into law by the federal legislature.

Under VAO, an authority ("VAO Authority") is to be established by the Federal Government for the licencing, regulation and supervision of virtual assets and virtual asset service providers. Virtual assets are defined as digital representation of value that can be digitally traded and used for payment or investment purposes but do not include digital representations of fiat currency, securities or other financial assets regulated under any other law. Virtual assets services include a range of services in relation to virtual assets including but not limited to exchange services, broker dealer services, advisory services, management and investment services etc. Issuers of virtual assets are deemed as virtual asset service providers if they offer the issued virtual asset to the public or third parties on a commercial basis. VAO requires that any person engaging in the provision of any virtual asset service, must be a company registered under the Companies Act, 2017 and hold a valid licence under VAO.

VAO Authority is required, inter alia, to ensure compliance of data protection and cyber security laws by virtual asset service providers; protect customers and investors dealing in virtual assets; establish and enforce standards relating to cybersecurity, data protection, risk management and technological safeguards for virtual asset activities; combat money laundering, terrorist financing and other illicit activities; establish and operate a regulatory sandbox for fostering innovation in virtual asset products and services etc. There are also restrictions on advertising or marketing (with prescribed disclosures) a fiat referenced token or an asset-referenced token. There are also obligations on issuers of virtual assets, including being licensed by VAO Authority, and issuing white papers in prescribed form and details prior to making an offering.

Penalties for violations of VAO can reach up to PKR 100,000,000/- or 5 % of the virtual service provider's annual turnover (in case of an issuer, 5% of the total value of the virtual asset offering), whichever is higher, and prison sentence of up to 7 years.

28. Search Engines and Marketplaces – Please summarise the principal laws (present or impending), if any, that govern search engines and marketplaces, including a brief explanation of the general purpose of those laws.

There are several laws that impact search engines and marketplaces.

- ETO is the basic law that facilitates electronic market places and e-commerce as it grants legal recognition and admissibility to documents, records, information, communication and transactions in electronic form. ETO gives recognition to electronic signatures as valid and enforceable, subject to certain reliability criteria. Contracts, invoices, receipts, and other business records in electronic form are treated as legally valid. Agreements made via websites, apps, or email are thus enforceable under Pakistani law.
- ETO also indirectly affects search engines, as content indexed or displayed by search engines—such as web pages, online publications, and digital advertisements—has legal recognition as electronic records. ETO recognises electronic agreements and communications and hence recognises clickwrap contracts or automated bidding systems involved in search-based advertising.
- Under the Telecom Act search engines and marketplaces can be issued directives by PTA in relation to platforms regarding content and access control.
- Pakistan also introduced the E-commerce Policy of Pakistan, 2019 which called for the regulation of online marketplaces, seller verification, consumer rights and dispute resolution mechanisms.
- Under PECA (and rules made thereunder) search engines and marketplaces must comply with provisions related to data retention, content takedown and cooperating with law enforcement.
- There is also the Digital Presence Proceeds Tax Act, 2025 whose ostensible purpose is to tax online marketplaces (both local and foreign) selling goods and services to Pakistani customers, especially those with little or no physical presence in Pakistan. To broaden the tax net to cover digital transactions, including e-commerce sales, digital payments, and advertising revenues from foreign platforms.
- The Digital Nation Pakistan Act, 2025 has been recently enacted with the object to transform Pakistan into a digital society and economy with robust digital governance. This establishes policy making and governance bodies like the National Digital Commission and Pakistan Digital Authority for strategic oversight and implementation of digital policies such as the National Digital Masterplan as a comprehensive, strategic blueprint designed to

transform Pakistan into a digital nation by fostering a digital society, digital economy and digital governance.
- Recently, the Finance Act, 2025 has amended the Income Tax Ordinance, 2001 to include new provisions for Ecommerce, by adding the definitions of e-commerce platforms and 'digitally delivered services'. e-commerce now includes the 'sale or purchase of goods and services' through 'websites, mobile applications or online marketplaces'.
- Once the Data Protection Bill is enacted into law, search engines and marketplaces will have to comply with its provisions relating to collection, storage and processing of user data.

29. Social Media – Please summarise the principal laws (present or impending), if any, that govern social media and online platforms, including a brief explanation of the general purpose of those laws?

PECA is the principal law that regulates social media. Its recent amendment through Prevention of Electronic Crimes (Amendment) Act, 2025 introduces controls over social media platforms and online content in Pakistan. It also established the Social Media Protection and Regulatory Authority ("SMPRA"), which is empowered to regulate social media platforms, (including the power to register and enlist them) ensure online safety, and regulate unlawful or offensive content on social media platforms accessible from Pakistan. SMPRA can block or remove content deemed unlawful or offensive, including content against ideology of Pakistan, or that incites violation of law or with a view to coerce, intimidate or terrorise, or that incites public to cause damage to governmental or private property, or coerces or intimidates public preventing them from carrying on lawful trade and disrupts civic life, or incites hatred and contempt on religious, sectarian or ethnic basis to stir up violence or cause internal disturbance, or contains anything obscene or pornographic in contravention of any applicable law, or is known to be fake, or false or there exist sufficient reasons to believe that the same may he fake or false beyond a reasonable doubt, or contains aspersions against any person including members of Judiciary; Armed Forces, Majlis-e-Shoora (Parliament) or a Provincial Assembly, or promotes and encourages terrorism and other forms of violence against the State or its institutions. PECA makes spreading false or fake information punishable by up to three years imprisonment and/or fines up to PKR 2,000,000/-. It also creates the Social Media Protection Tribunal to oversee cases regarding social media.

The rules made under PECA, inter alia, envisage registration with PTA of significant social media platforms i.e., platforms with over a half a million users. These rules also envisage social media platforms to deploy mechanisms to ensure immediate blocking of live streaming of any online content particularly relating to terrorism, hate speech, pornographic, incitement to violence and detrimental to national security on receiving intimation from the Authority.

Digital Nation Pakistan Act, 2025 is a law that complements PECA supporting the broader digital governance framework, including the regulation of digital platforms, enhancing cybersecurity, and promoting digital transformation.

30. Social Media – What is the maximum sanction that can be imposed by a regulator in the event of a breach of any applicable online safety laws?

PECA empowers the courts to sanction a range of offences. The following are of note:

a. posting false and fake information – maximum of 3 years imprisonment and/or a fine of up to PKR 2,000,000/-
b. glorification of an offence – a maximum of 7 years imprisonment and/or a fine of up to PKR 10,000,000/-
c. cyber terrorism – maximum of 14 years imprisonment and/or a fine of up to PKR 50,000,000/-
d. hate speech – maximum of 7 years imprisonment and/or a fine.
e. recruitment, funding and planning of terrorism – maximum of 7 years imprisonment and/or a fine.
f. electronic fraud – maximum of 2 years of imprisonment and/or a fine of up to PKR 10,000,000/-
g. unauthorised use of identity information – maximum sanction of 3 years of imprisonment and/or a fine of up to PKR 5,000,000/-
h. against the dignity of a natural person – maximum of 3 years imprisonment and/or a fine of up to PKR 1,000,000/-
i. against the modesty of a natural person and minor – maximum of 10 years and/or a fine of up to PKR 5,000,000/-.
j. production, offering or making of child pornography – maximum of 20 years imprisonment and a fine of at least PKR 1,000,000/-
k. online grooming, solicitation and cyber enticement – maximum of 10 years imprisonment and a fine up to PKR 10,000,000/-
l. use of information systems for commercial

exploitation of children – maximum punishment of 20 years and a fine of at least PKR 1,000,000/-
m. using information system to kidnap, abduct or traffic a minor – maximum of 20 years imprisonment and a fine of at least PKR 1,000,000/-
n. cyber stalking – maximum of 3 years imprisonment and/or a fine of PKR 1,000,000/-, provided if the person stalked is a minor, the sanction increases to imprisonment up to 5 years and/or a fine of PKR 10,000,000/-
o. cyberbullying – maximum of 5 years imprisonment and/or with a fine of up to PKR 500,000/-
p. spamming – maximum of 3 months imprisonment and/or a fine of up to PKR 5,000,000/-
q. spoofing – maximum of 3 years imprisonment and/or a fine of up to PKR 500,000/-

31. Spatial Computing – Please summarise the principal laws (present or impending), if any, that govern spatial computing, including a brief explanation of the general purpose of those laws?

There are at present no laws that govern spatial computing in Pakistan.

32. Quantum Computing – Please summarise the principal laws (present or impending), if any, that govern quantum computing and/or issues around quantum cryptography, including a brief explanation of the general purpose of those laws?

There are at present no laws that govern quantum computing in Pakistan.

33. Datacentres – Does your jurisdiction have any specific regulations that apply to data centres?

There is a patchwork of laws, regulations, and policies across multiple sectors that might apply, including PECA, which criminalises unauthorised access and transmission of data; the draft Data Protection Bill, which mandates consent-based processing, restricts cross-border data transfers, and requires localisation of critical personal data; the Critical Telecom Data and Infrastructure Security Regulations, 2020 issued by PTA which prescribe cybersecurity and physical safeguards for telecom infrastructure; the Computer Emergency Response Team Rules, 2023 which establishes Pakistan's national computer emergency response team, and requires incident response mechanisms for critical infrastructure; SBP's BPRD Circular No. 06 of 2019 governing outsourcing by financial institutions, including data centre services; the Cloud-First Policy, 2022 issued by MOITT, which promotes cloud computing and supports public cloud infrastructure including data centres; the Special Technology Zones Authority Act, 2021 which facilitates the development of high-tech infrastructure such as data centres in designated zones.

34. General – What are your top 3 predictions for significant developments in technology law in the next 3 years?

A. Pakistan is likely to enact and operationalise the Data Protection Bill, creating a legal framework for data privacy, localisation, and cross-border transfers in the country. We understand that MOITT is currently in the process of reviewing and updating the latest draft, with a view to pushing it through the legislative process. The final version is expected to be modelled closely on EU GDPR, and will likely include the creation of a dedicated regulatory authority to oversee compliance and enforcement. This development will have far-reaching implications for the broader technology, media, and telecommunications landscape in Pakistan. Businesses will be required to revise their data collection and retention practices, implement breach notification mechanisms, and establish protocols for international data transfers. Most notably, the introduction of a robust data protection regime could enhance Pakistan's standing as a trusted outsourcing destination, particularly among European Union member states and other jurisdictions with stringent data protection standards.
B. Pakistan is likely to develop a comprehensive AI regulatory framework. The current national AI policy is likely to evolve into enforceable guidelines or legislation, addressing critical issues such as AI ethics, liability, algorithmic transparency, and accountability. In parallel, emerging technologies closely linked to AI—such as cloud hosting, smart contracts, and tokenisation—may also be brought under regulatory scrutiny, particularly within the fintech and govtech sectors. This shift is expected to prompt significant updates to existing IT, banking, and public procurement regulations, aligning them with the demands of an increasingly automated and data-driven environment. We also note that AI will likely also have a significant impact on the legal sphere.
C. VAO appears a clear signal that Pakistan intends to provide a legal framework for the

blockchain/crypto/virtual asset market. The government had been talking increasingly about the importance of regulating the burgeoning crypto industry, and the formation of PCC and PDAA, and the introduction of VAO all indicate that a law passed by the federal legislature to regulate crypto is imminent.

D. We also anticipate increased coordination among PTA, SBP, and MOITT to develop a harmonised national cybersecurity framework, potentially aligned with international standards such as ISO/IEC 27001 or those developed by the National Institute of Standards and Technology. Much like the expected data protection reforms, this initiative would have a significant impact on corporate governance and compliance policies across sectors in Pakistan. The introduction of a unified cybersecurity regime would likely compel larger legal entities to strengthen their internal security protocols, invest in robust risk management systems, and adopt industry-standard safeguards. Over time, this could substantially elevate Pakistan's overall cybersecurity posture and enhance trust in its digital infrastructure.

35. General – Do technology contracts in your country commonly include provisions to address sustainability / net-zero obligations or similar environmental commitments?

Not at the moment but this might change soon.

Contributors

Aneeq Shah
Associate
aneeq.shah@chima-ibrahim.com

Yasser Hamdani
Senior Counsel
yasser.hamdani@chima-ibrahim.com

Ali Asim
Partner
ali.asim@chima-ibrahim.com

Shazil Ibrahim
Partner
shazil.ibrahim@chima-ibrahim.com