COUNTRY COMPARATIVE GUIDES 2020

The Legal 500 Country Comparative Guides

Philippines
TECHNOLOGY

Contributing firm

Gorriceta Africa Cauton & Saavedra

Mark S. Gorriceta

Managing Partner and Head of Corporate Group | msgorriceta@gorricetalaw.com

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

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

PHILIPPINES
TECHNOLOGY

1. What is the regulatory regime for technology?

The provision of Information Technology services/solutions in the Philippines is generally unregulated, unless such I.T. services/solutions involve any of the following:

- banking, remittance, electronic money, electronic payment systems, virtual currency conversion, and prospectively, virtual assets & virtual asset service providers under the regulation of the Bangko Sentral ng Pilipinas (Philippine Central Bank or "BSP");
- crowdfunding and, prospectively, digital asset offerings and digital asset exchanges under the regulation of the Securities and Exchange Commission ("SEC");
- telecommunications under the regulation of the National Telecommunications Commission ("NTC");
- data privacy and personal data processing under the regulation of the National Privacy Commission ("NPC");
- insurance and insurance products under the regulation of the Insurance Commission ("IC");
- telemedicine in light of the COVID-19 pandemic under the joint-regulation of the Department of Health ("DOH") and the NPC;
- transport network companies and transport network vehicle services under the Land Transportation Franchising and Regulatory Board ("LTFRB");
- consumer protection and loyalty rewards under the regulation of the Department of Trade and Industry ("DTI");
- general logistics and fulfilment services operating as an authorized Private Express and/or Messengerial Delivery Service ("PEMEDES") or Courier Service Provider under the Department of Information and Communications Technology ("DICT");
- anti-money laundering mechanisms under the regulation of the Anti-Money Laundering Council ("AMLC") in coordination with the BSP (for BSP-supervised financial institutions) and the SEC (for SEC covered entities);
- cybersecurity and cybercrime under the joint regulation of the NTC, NPC, DTI, DICT, Philippine National Police ("PNP"), National Bureau of Investigation ("NBI"), and the Department of Justice ("DOJ"); and
- prospectively for online e-commerce and media streaming platforms, a proposal by the Bureau of Internal Revenue ("BIR") to subject such platforms to Philippine tax laws regardless of the platform owner's domicile for so long as the platform services are availed of in the Philippines.

Finally, the Philippines' Information Communications Technology ("ICT") policy formulation, planning, coordination, and implementation shall be under the helm of the DICT in partnership with the above-mentioned entities.

2. Are communications networks or services regulated?

Telecommunications networks or services are generally covered by the Public Telecommunications Policy Act of the Philippines ("Telecoms Act"). It further establishes the NTC – the government agency tasked with administering telecommunications regulations.

Telecommunications networks or services are matters of public interest and are classified as public utilities. Thus, as a public utility, the Philippine Constitution limits foreign equity ownership to (40%).

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

The Telecoms Act primarily regulate the following activities: (i) telecommunications; (ii) broadcasting; (iii) Value Added Services; and (iv) Voice over Internet

Protocols Services, respectively defined as follows:

- Telecommunications pertain to “any process that enables a telecommunications entity to relay and receive voice, data, electronic messages, written or printed matter, fixed or moving pictures, words, music or visible and audible signals or any control signals of any design and for any purpose by wire, radio or other electromagnetic, spectral, optical or technological means”;
- Broadcasting pertains to “an undertaking the object of which is to transmit over-the-air commercial radio or television messages for reception of a broad audience in a geographical area”;
- Value-Added Service (“VAS”) providers are “entities, which relying on the transmission switching, and local distribution facilities of the local exchange and inter-exchange operators and overseas carriers offer enhanced services beyond those ordinarily provided for by such carriers.”
- Voice Over Internet Protocol (“VoIP”) Services pertain to the “provision of voice communication using Internet Protocol technology, instead of traditional circuit switched technology.”

An entity which provides telecommunications and/or broadcasting services is a Public Telecommunications Entity (“PTE”). Prior to operation, a PTE aspirant must first obtain a legislative franchise from Congress as well as a Certificate of Public Convenience and Necessity (“CPCN”) from the NTC before it can engage in any telecommunications or broadcasting activities. For PTEs with wireless or mobile services, they must also request a frequency assignment from the NTC. Finally, VAS and VoIP providers are required to secure a Certificate of Registration from the NTC.

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

The NTC is the principal regulatory body for communications-related services. Aside from the NTC, the Movie and Television Review and Classification Board (“MTRCB”), the Optical Media Board (“OMB”), the National Council for Children’s Television, and the Kapisanan ng mga Brodkaster ng Pilipinas (“KBP”) likewise perform regulatory oversight when it comes to media and broadcasting activities.

Aside from the above, other regulatory bodies such as the SEC (corporate and securities regulation), DTI (consumer protection), and DICT (ICT matters) may likewise regulate providers of communications-related services for activities covered by their respective jurisdictions.

5. Are they independent of the government control?

In general, grantees of telecommunications franchises are free from government control and censorship as to the content of matters broadcasted, provided that the speech, play or other matters being broadcasted are not contrary to laws (i.e., must not propose and/or incite treason, rebellion or sedition) or public morals (i.e., that the language used therein or the theme thereof is not indecent or immoral).

Further, as telecommunication providers are considered public utilities, there are statutory limits with respect to foreign equity ownership as well as the number of broadcast stations and channels a single entity may own, operate or manage. Congressional franchise grants to operate telecommunication systems are also constrained with time limits, subject to an application for renewal of the said franchise. Moreover, radio and television channels are mandated to allocate at least two (2) hours a day for public service programs and to also provide an access channel for the use of specific entities, such as the National Government and socio-civic organizations, free of charge as a public service feature of the television cable systems.

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

I.T. platform providers for social media, content sharing, and information search engines are generally not regulated. However, for data processing activities of the said platform providers, they must comply with the Data Privacy Act (“DPA”), its implementing rules and regulations, as well as the issuances of its primary regulator: the NPC. Platform providers that distribute content through telecommunications entities or provide voice communication using Internet Protocol technology, instead of traditional circuit switched technology must also register with the NTC as VAS and VoIP providers, respectively.

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

For data privacy matters, the DPA provides for extra-territorial application with respect to data processing activities when (i) it relates to the personal information of Filipino citizens/residents and/or (ii) when the entity has a link with the Philippines (i.e., by way of contract, business operations, access with the personal information held by a Philippine entity, etc.). Thus, the NPC can extend its regulatory powers for activities outside of Philippine territory under these circumstances.

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

Yes. Under the Philippine Constitution, as an entity operating a public utility, a telecoms operator must be a Philippine citizen or entity organized under the laws of the Philippines. This will entail being domiciled in the Philippines.

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

Yes. Under the Philippine Constitution, as an entity operating a public utility, a telecoms operator must be a Philippine citizen or entity organized under the laws of the Philippines with a maximum of forty percent (40%) foreign ownership.

Furthermore, for a telecoms operator engaged in mass media activities (i.e. radio, television, and cable TV broadcasting), it must be fully-owned by Filipino citizens or, if a corporate entity, must have one hundred percent (100%) Filipino equity.

10. Are there any regulations covering interconnection between operators?

The Telecoms Act mandates a fair and reasonable interconnection of facilities of authorized public network operators and other providers of telecommunications services through appropriate modalities of interconnection and at a reasonable and fair level of charges. Thus, interconnection is mandatory. Further, telecoms operators are required to negotiate and execute interconnection agreements as well as publish reference access offers as default offers to prevent any anti-competitive behavior.

The NTC checks on anti-competitive behavior of PTEs by enforcing fair pricing and reasonable interconnection, among other requirements under Philippine regulations.

The recently passed Mobile Number Data Portability Act likewise provides a nationwide Mobile Number Portability ("MNP") system which gives consumers the freedom to choose and to respond to quality, price, and other relevant considerations without the consumers having to change their mobile numbers whenever they switch to another mobile service provider or subscription plan. In this regard, PTEs are required to set up a mechanism for the implementation of the MNP system which shall interconnect directly or indirectly with the infrastructure, facilities, systems, or equipment of other PTEs and not install network features, functions or capabilities that will impede the implementation of the nationwide MNP system.

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

In general, the regulations covering interconnection between operators do not differ between operators with and without market power as all modalities of interconnection must be at reasonable and fair levels of charges. However, the Philippine Competition Act ("PCA") prohibits entities from abusing their dominant position in the market by engaging in conduct that would substantially prevent, restrict, or lessen competition.

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

Telecoms entities are required to comply with general pricing principles established by the NTC which in essence balances anti-predatory pricing principles through tariff schedules vis-à-vis a fair return of the telecom operators' investments to be economically viable considering the prevailing capital cost in domestic and international markets.

For telecom operators providing telephone services, they should state charge options for the supply of consumer access services; meanwhile, internet access providers must inform subscribers of their minimum connection speed and service rates, and maintain service availability above the minimum connection speed 80% of the time for every month of subscription.

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

The Intellectual Property Code protects the rights of software developers by allowing them to obtain a copyright for the programs they develop. A copyright is the legal protection extended to the owner of the rights

in an original work. 'Original work' refers to every production in the literary, scientific and artistic domain which can include computer software (i.e. source codes).

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

Yes. Data/databases – provided that they are classified as 'original work' – are works covered by copyright under the Intellectual Property Code. While not required, owners of copyrighted work may deposit their works either with the National Library or the Intellectual Property Office.

15. What key protections exist for personal data?

The Data Privacy Act, its implementing rules and regulations, and issuances by the NPC (collectively, "Philippine Data Privacy laws") allow the processing of personal data subject to the principles of transparency, legitimate purpose, and proportionality. Based on these principles, personal data must be: collected for specified and legitimate purposes; processed fairly and lawfully; accurate, relevant and kept up to date; adequate and not excessive in relation to the purposes for which they are collected and processed; and retained only for as long as necessary. Adequate technical, organizational, and physical safeguards must also be implemented in the course of the data processing.

For Personal Data Controllers ("PICs") or Personal Information Processors ("PIPs"), they are required to register with the NPC and appoint a Data Protection Officer which, primarily, must monitor the PIC's or PIP's compliance with Philippine Data Privacy laws. Registration of the Data Processing Systems ("DPS") is also required under the DPA; however, this has been currently suspended by the NPC pending the re-development of its online DPS registration portal.

In cases of personal data breach, the Philippine Data Privacy laws likewise require mandatory breach notifications to the NPC and the concerned data subjects in the event that the breach involves sensitive personal information or any information that can be used to perpetuate fraud. In such an event, the PIC/PIP must likewise facilitate the rectification or mitigation of the said data breach, in addition to potential fines and penalties that may be imposed under the law.

Notably, the NPC is clothed with the power to issue cease and desist orders and/or impose a temporary or permanent ban on the processing of personal information, upon finding that the processing will be detrimental to national security and public interest.

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

No. Personal data may be subject to cross-border transfers provided that the transfer of personal data is compliant with the requirements of the Data Privacy Act concerning data sharing/outsourcing arrangements (i.e. data subject's consent to such transfer has been validly obtained and technical, organizational, and physical safeguards are implemented by the offshore PIC/PIP). Notably, the PIC shall be primarily accountable for personal data under its control or custody, including information that have been transferred to a third–party (whether locally or offshore) for processing.

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

The maximum applicable fine for breach of data protection laws is a fine of Php 5 Million with imprisonment ranging from three (3) to six (6) years if the violator has committed a combination or series of acts constituting as punishable offenses under the DPA.

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

In essence, the DPA affords similar protections and responsibilities imposed by the GDPR, with a caveat of the latter having gone through more advanced implementation through institutions and regulations of the European Union.

In terms of penalties, however, note that the DPA can impose imprisonment as a penalty (aside from fines) whereas it is our understanding that the GDPR only imposes a fine of up to €20 Million or 4% of annual worldwide turnover of the responsible controller/processor, whichever is higher.

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

For public/governmental cloud-based services, the DICT has prescribed the Philippine Government's "Cloud First Policy". While the issuance mainly covers the government's transition into using cloud-based platforms, the implementation also covers private

entities that will participate as accredited Cloud Service Providers ("CSPs") of governmental institutions.

While the DICT has not yet prescribed the full accreditation procedure for CSPs, baseline requirements under the current DICT policy include:

a) Security Assurance Requirements in the form of:

1. ISO/IEC 27001 – Information Security Management
2. Payment Card Industry ("PCI") Data Security Standard

b) Service Level Agreements ("SLAs"), which must contain provisions on incentives, penalties, escalation procedures, disaster recovery and business continuity and contract cancellation for the protection of the institution, in the event the service provider fails to meet the required level of performance, among others.

Further technical and sector-specific certifications or requirements may likewise be imposed depending on the industry. For example, BSP Supervised Financial Institutions ("BSFIs") that outsource core IT services and functions via cloud computing platforms are required to subject their outsourcing arrangements to a higher degree of oversight, due diligence, and risk management controls.

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

Under the Electronic Commerce Act, an electronic signature on an electronic document shall be equivalent to the signature of a person on a written document provided that the electronic signature can be shown to have been made following a prescribed procedure, not alterable by the parties interested in the electronic document.

Specifically, the Electronic Commerce Act requires that the method for procuring the electronic signature: (i) can identify the signatory and his/her access to the electronic document; (ii) is reliable and appropriate for the purpose of the electronic document; (iii) is necessary in order to proceed with the transaction; and (iv) will authorize and enable the other signatory/ies to verify the electronic signature and to make the decision to proceed with the transaction authenticated by the same.

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

None. No automatic transfers of employees, assets, or third-party contracts to outsourcing suppliers for outsourced I.T. services are provided for under the law. However, this may be subject to commercial agreements, provided that applicable labor laws are likewise observed.

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

Since no laws with respect to Artificial Intelligence and software/operations in relation thereto are available at present, general rules on civil and criminal liability must be followed. In the example of a malfunctioning A.I. software which causes damage, this may be appreciated as a form of a negligent act which, if not meeting the standard of care required by law, would be attributable to its developer/operator.

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

The key laws in terms of obligations as to the maintenance of cybersecurity are following:

- Cybercrime Prevention Act – recognizes the need to protect and safeguard the integrity of computer, computer and communications systems, networks, and databases, and the confidentiality, integrity, and availability of information and data stored therein, from all forms of misuse, abuse, and illegal access by making punishable such conduct/s.
- Data Privacy Act – with respect to cybersecurity, the DPA prescribes and requires technical safeguards for the protection of personal data stored in electronic form.
- Electronic Commerce Act – requires appropriate security and authentication procedures for the authenticity electronic signatures and documents.
- Access Devices Regulation Act – protects the rights and defines the liabilities of parties in commercial transactions involving 'access

devices' (defined as any electronic means to obtain money, good, services, or any other thing of value or to initiate a transfer of funds) by regulating the issuance and use of access devices.

- Anti-Wiretapping Law – prohibits and penalizes wiretapping and other related violations of the privacy of communication.

With respect to the criminality of hacking, the applicable law would be the Cybercrime Prevention Act which prohibits and penalizes cybercrimes. Depending on the intent and acts performed in relation to the hacking activity, it may be considered as (i) offenses against the confidentiality, integrity and availability of computer data and systems, i.e. illegal access, interception, interference, etc. or (ii) computer-related offenses, i.e. computer-related forgery, fraud, identity theft, etc.

With respect to Distributed Denial-of-Service("DDoS") attacks, this may likewise be classified under the Cybercrime Prevention Act as an offense against the confidentiality, integrity and availability of computer data and systems. Specifically, this may be punishable as 'system interference' which is defined as an "intentional alteration or reckless hindering or interference with the functioning of a computer or computer network by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data or program, electronic document, or electronic data message, without right or authority, including the introduction or transmission of viruses."

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

In light of the COVID-19 pandemic which has greatly amplified the need for digitization across systems and institutions in the Philippines (and of course, globally), the following technological developments/infrastructures will bring about the most changes:

- Digitization of frontline government services. Government institutions, through the general oversight of the DICT, must immediately transition and/or provide digital alternatives to frontline services in order to expedite these processes and avoid disruption of public services. An example of this is the newly launched eGov Pay facility which provides the public a payment solution for the streamlined digitization of government collections and disbursements.
- The implementation of the National I.D. System. Under the Philippine Identification System Act, there shall be a single national identification system ("PhilSys") for all citizens and resident aliens of the Philippines. This is key to the Philippine digital economy roadmap as it allows for the seamless integration of the government's services and the accessibility of financial services through the recognition of a single valid proof of identity ("PhilSys ID") by public and private institutions.
- The creation of digital banks and proliferation of digital payment systems/infrastructures. While duly licensed banks may provide for digital banking services, laws and/or regulations towards a fully digital bank have yet to be issued. The BSP has already issued its draft Guidelines on the Establishment of Digital Banks. Once in final form, we expect new and progressive players in the financial sector that can help speed up the financial inclusion of the underbanked and unbanked sectors of Philippine society.
- Blockchain technology. To date, only Virtual Currency Exchange ("VCE") platforms which allow the conversion of virtual currencies to fiat (and vice-versa) are DLT-brought services which are regulated by the BSP. The SEC, while it has already issued proposed rules on Digital Asset Offerings and Digital Asset Exchanges more than a year since, have yet to issue official regulations thereof. Aside from these services, the rise of blockchain technology on its own can offer multi-sector solutions to pain points in today's Philippine economy, such as in record-keeping, financial services accessibility, supply chain solutions, etc.
- Crowdfunding platforms. Serving as an intermediary portal between investors and issuers of debt or equity securities, the SEC's Crowdfunding Rules provides for alternative modes of financing especially for the Micro, Small and Medium Enterprises ("MSMEs"). While no entity has been granted a crowdfunding license as of date, a duly licensed Crowdfunding Platform can stimulate the private sector and provide much needed capital in these times of recession.

25. Which current legal provision/regime creates the greatest impediment to

economic development/ commerce?

The following underdeveloped or non-existent legal regimes creates impediment to economic development/commerce:

- Broad interpretation of “mass media activities”. As per the DOJ, ‘mass media’ refers to “any medium of communication designed to reach the masses and that tends to set the standards, ideals and aims of the masses, the distinctive feature of which is the dissemination of information and ideas to the public, or a portion thereof.” Note that entities engaged in mass media activities must be fully owned by Filipino citizens. In light of the digital economy with platforms catering to a marketplace of ideas, a broad interpretation of what constitutes as ‘mass media’ can cause confusion and/or risk-aversion in the entry of foreign capital into domestic entities operating digital platforms.
- Lack of fully–digital banking regulations. Presently, to offer digital banking services, once must first secure a traditional banking license with the BSP (i.e., universal bank, commercial bank, etc.) and then apply for approval to offer such banking services via digital means/platforms. Thus, a direct application to be a fully digital bank is not yet available to date. However, BSP has recently issued the draft guidelines on establishments of digital banks which would allow offering of financial products and services through digital platforms or electronic channels with minimal reliance on physical touchpoints. The finalization of the said rules will substantially contribute to BSP’s digital payments transformation roadmap.
- Stalling of the passing of the Digital Asset Offering and the Digital Asset Exchange Rules. The SEC has already issued the proposed DAO and DAE Rules in 2018 and 2019, respectively. The private sector invested in blockchain technology has long awaited for these rules to be finalized in order to explore alternative modes of fundraising and benefit from the steady growth and utility of digital assets across the globe.
- Lack of defined FinTech Sandbox Rules. Unlike Singapore and its FinTech Regulatory Sandbox under the Monetary Authority of Singapore, the Philippines does not have a fixed set of sandbox rules for the FinTech industry. Instead, this is pursued on a per regulator basis wherein each agency, subject to the limits of key laws and regulations, may each prescribe for their own “sandbox licenses” or approach at their discretion. For example, the BSP has been more progressive in awarding sandbox licenses for innovative technologies and platforms involving fiat and payment facilities not squarely falling under its current set of BSP licenses. On the other hand, the SEC has pursued a more conservative approach by limiting sandbox approvals to stringent conditions pursuant to prevailing laws (i.e., the Securities Regulation Code) or by altogether banning activities which are currently not subject of any official regulation (i.e. Digital Asset Exchanges).

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

The Philippine legal system, subject to the balancing of consumer protection principles, generally encourages digital services in the country. This can be seen through the passage of the Philippine Innovation Act and the Innovative Startup Act. The former provides for a comprehensive support program to promote MSME innovation through the establishment of an Innovation Fund, while the latter created a regime to protect and promote innovative products, processes, and business models as well as provides for a Startup Venture Fund.

In addition to fostering a conducive climate for innovation and startup building, the Philippines has also taken an active role in the Asian region in embracing digital innovations such as blockchain technology (through the regulation of VCEs and, prospectively, DAOs and DAEs), crowdfunding platforms, and developments in digital financial services (i.e. electronic money, payment systems, etc.).

Further, forthcoming digital economy-friendly laws such as the Internet Transaction Act and the National Digital Careers Act are on its way. If passed, the Internet Transaction Act seeks to create an eCommerce Bureau which shall handle the online dispute resolution platform for consumers, online merchants and traders. Meanwhile, again if passed, the National Digital Careers Act seeks to protect and strengthen the digital and online freelance industry, institutionalize employments standards for digital career workers and enhance their competitiveness through access to necessary trainings, skills development and scholarship programs.

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

Artificial Intelligence has yet to be specifically governed by any law in the Philippines. Plausibly, the initial regulations may likely be introduced by the BSP for financial services and/or by the SEC for AI-powered financial/securities-related platforms/services (i.e. payment systems, robo–advisory). In which case, as these entities only have delegated powers under the law, their regulations are still subject to key and traditional laws governing financial services (i.e. the New Central Bank Act) and securities (i.e., Securities Regulation Code).

Contributors

Mark S. Gorriceta
Managing Partner and Head of Corporate Group
msgorriceta@gorricetalaw.com