Legal 500
Country Comparative Guides 2026

Philippines
TMT

Contributor

Vasig Abarquez Ner
Urgello & Lim

Maria Pia A. Urgello

Senior Partner | piaurgello@val.law

Mary Aubbrey B. Lim-Barreras

Senior Partner | aubbreylim@val.law

Reeneth B. Santos

Junior Partner | reenethsantos@val.law

Mitchel Q. Tuazon

Junior Partner | mitchel.q.tuazon@val.law

Anna Rochelle D. Payongayong

Junior Associate | annapayongayong@val.law

Lesley Ysabel B. Sumagpang

Junior Associate | lesleysumagpang@val.law

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

Philippines: TMT

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

Proprietary rights in software and associated materials in the Philippines are protected under Republic Act No. 8293, otherwise known as the Intellectual Property Code of the Philippines (IP Code).

Software is protected automatically from the moment of creation as "computer programs" classified as original literary works under the law on copyright. Meanwhile, the visual and the branding elements of the software, such as its name, logo, and application icons, are protected against unfair competition and brand confusion under trademark law, subject to registration with the Bureau of Trademarks of the Intellectual Property Office of the Philippines.

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?

The determination of the ownership of a copyright is governed by the IP Code, which provides that in a case of work commissioned by a person other than an employer of the author and who pays for it and work is made in pursuance of the commission, the person who commissioned the work shall have ownership of the work. However, the copyright thereto shall belong to the author of the work.

In the case of work created by an author or developer during and in the course of employment, the copyright shall belong to the employee, if the creation of the object of copyright is not part of his regular duties even if the employee uses the time, facilities, and materials of the employer. On the other hand, the employer will own the copyright if the work is the result of the performance of the employee's regularly assigned duties.

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

While not specific or limited to software or computer systems, the following laws govern in case of harm/defect caused by software/computer systems:

1. Republic Act No. 10173 also known as the Data Privacy Act of 2012, if a system failure or defective software results in personal data leaks or unauthorised personal data exposure
2. Republic Act No. 11967 also known as the Internet Transactions Act of 2023, if e-commerce platforms' system failures result in harm to online consumers. The law imposes various obligations on digital platforms, e-marketplaces, and online merchants to ensure secure, reliable, and transparent internet transactions. Where a platform failure results in inability to verify merchant information, process payments or orders, facilitate communication between merchants and consumers, fulfil purchases, or ensure that the goods and services conform to the descriptions, quality, safety standards, and warranties made to consumers, the resulting harm may fall within the scope of obligations imposed on e-marketplaces, online merchants, and e-retailers under the Act.
3. Republic Act No. 7394 also known as Consumer Act of the Philippines, if damage is caused to consumers by reason of defective software products.
4. Republic Act No. 10175 also known as Cybercrime Prevention Act of 2012, which requires providers to preserve certain computer data, including content, traffic data and subscriber information for the period prescribed by law. It likewise imposes obligations on service providers to cooperate with lawful investigations by preserving and disclosing relevant data and providing necessary technical assistance in accordance with court-issued warrants.

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?

When a software is used or misused to cause harm, the following laws may apply:

1. Cybercrime Prevention Act of 2012 in cases of system or data interference, or procurement of software designed primarily to commit cybercrimes. Convicted individuals may face a prison sentence of prison mayor, spanning six (6) years and one (1) day to 12 years, and may likewise be subject to the fines prescribed by law. However, if these acts target the nation's critical infrastructure, the penalty escalates to reclusion temporal, increasing imprisonment to 12 years and one (1) day to 20 years, with the corresponding fines prescribed by law. Furthermore, where the act is committed for the benefit of a juridical entity, corporate liability may attach, and the corporation may be subjected to a fine of up to PhP10,000,000.
2. Republic Act No. 8792 also known as the Electronic Commerce Act of 2000 in case of interference in a computer system/server or information in order to corrupt, alter, steal or destroy using a computer or other similar information and communication device. The penalty imposed under this law is six (6) months to three (3) years of imprisonment and a minimum of PhP 100,000. However, the Cybercrime Prevention Act of 2012 may instead be used for the exact same offense to enforce harsher penalties.

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?

IP Code dictates that software license, or SaaS subscription is merely a limited grant of usage rights, while the vendor inherently retains the copyright.

For vendors that provide cloud services, they should consider the data ownership, data classification and data sovereignty rules that are deemed automatically incorporated in their agreements with the Philippine government. Please see further discussion in question #35.

Electronic Commerce Act of 2000, on the other hand, serves as the statutory foundation that makes the operation mechanics of digital licensing and SaaS delivery possible. The law explicitly provides electronic contracts and end-user license agreements the same legal status and biding effect as traditional contracts.

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 commercial practice for software vendors to limit their liability. The liability caps are often calculated based on fees paid over a short duration; for example, service fee for the month during which the loss or breach occurred, or one (1) year before the events or circumstances occurred, or if the service is free, up to a small capped amount.

If not a specific cap amount, the limitations of liability would also often exclude as part of limitation of liability the consequential losses; loss of profits or income, whether actual or anticipated; and loss of goodwill or business reputation.

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; (h) claims arising out of or in relation to artificial intelligence.

Software license agreements generally do not include these specific general exclusions to the financial liability cap. Rather, the agreements would generally rely on catch-all phrases like "to the extent permitted by applicable law" or "except for statutory liabilities that cannot be excluded under the law".

However, we have seen license agreements were data protection breaches and data security breaches are subject to a separate enhanced cap in a negotiated transaction, and at the insistence of customers, due to the subject matter involved. Breaches and loss of data

may also result in financial and reputational harm to the customers and the enhanced cap accounts for this.

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?

Source code escrow is prevalent in the Philippines, especially in the banking sector. Since banks are mandated to conduct business continuity and strict technology risk assessment, local banks generally execute escrow agreements. However, due to lack of highly specialized local tech escrow firms in the country, Philippine enterprises generally use international providers with global infrastructure.

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

Under the Data Privacy Act of 2012, in Information Technology (IT) outsourcing or subcontracting arrangements involving personal data handling, the vendor may be considered as a personal information controller (PIC) if it exercises independent decision-making power over the personal data by determining the purposes and means of processing, including establishing retention schedules. As a PIC, it has the responsibility of ensuring proper safeguards to ensure confidentiality of the personal information processed.

On the other hand, a vendor would be classified as a personal information processor (PIP) where they handle personal data solely on behalf of, and under the documented instruction of, the customer who remains the primary PIC, such as in cloud hosing or standard SaaS applications. In the event of a personal data breach involving sensitive information, the primary obligation falls on the PIC, who must notify both the National Privacy Commission (NPC) and the affected data subjects within a strict deadline from the discovery of the breach, the notification shall at least describe the nature of the breach, the sensitive personal information possibly involved, and the measures taken by the entity to address the breach.

For transactions in the regulated financial sector, BSP's Manual of Regulations for Banks (MORB) provides regulations on outsourcing and IT risk management granting the BSP the right to audit and physically inspect the vendors' security control mechanism. Under MORB, the requirement for prior BSP approval depends on the bank's Supervisory Assessment Framework (SAFr) composite rating and the materiality of the IT function:

- A BSP-supervised Financial Institution (BSFI) must secure prior written approval from the appropriate supervising department of the BSP before implementing or making significant changes to a material IT outsourcing arrangement, if the bank's SAFr composite rating is below '3'. This material outsourcing arrangement covers new material outsourcing arrangements, changes in existing material outsourcing arrangements that have significant impact in the delivery of outsourcing services, business operations, reputation and profitability, or changes in existing outsourcing arrangements resulting in the reclassification of the arrangements as material such as, but not limited to those affecting the nature, scope, and complexity of systems and processes.
- If the BSFI maintains a stable SAFr composite rating of at least '3', it is allowed to proceed with material IT outsourcing without prior BSP approval, provided, it submits a formal notification letter, a board -approved materiality assessment and compliance certifications to the BSP. However, no bank or BSFI can outsource inherent banking function, such as taking of deposits from the public; granting of loans and extension of other credit exposures, managing of risk exposures, and general management.

Additionally, at a minimum, the contract should contain the following provisions: i) the BSFI retains exclusive ownership over all of its data; ii) the third-party service provider (TSP) acquires no rights whatsoever to use the BSFI's data for its own purpose or for any purpose other than what is required based on the scope of service; and iii) the TSP does not have the right to prevent the duly authorised access of BSFI to its own data. For these provisions to work as intended, the terms of data ownership must not be subject to unilateral amendment by the TSP.

10. 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 the Labor Code of the Philippines (Labor Code), installation of labour-saving devices and redundancy are recognized as lawful causes to terminate employment. The purpose of this law is to recognise management prerogative, subject to payment of separation pay to the terminated employee. When an enterprise transfers a service to a third-party IT outsource provider, resulting in termination of employment of an employee, the employer must comply with due process requirements i.e., notice to the affected individual and the labour authority, and payment of legally mandated separation pay. Failure to comply with both substantive and procedural due process may render the termination illegal and would expose the employer to penalties.

The Labor Code likewise prohibits diminution of benefits, ensuring that employees retain the benefits given by employers, protecting employees from reduction in compensation structure by reason of corporate restructuring or service transfers.

11. 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.

Article XII, Section 11 of the Philippine Constitution restricts the operation of public utilities (which previously included all telecommunications) to entities at least 60% owned by Filipino citizens. This also affirms the state's authority to regulate these services in the public interest.

The primary legislation is Republic Act No. 7925 or the Public Telecommunications Policy Act, which serves as the cornerstone law establishing policies to promote fair competition, private investment, and universal access to telecommunications services, while mandating the National Telecommunications Commission (NTC) to regulate the industry and ensure reasonable pricing.

Republic Act No. 3846 or the Radio Control Act, is a longstanding law which regulates radio stations and radio communications. It mandates that no entity shall construct or operate a radio transmitting or receiving station for commercial purposes without obtaining a franchise. It also empowers the regulatory body (now the NTC) to allocate frequencies, issue necessary licences, and prevent signal interference.

Another principal law is Republic Act No. 11659, which amends the Public Service Act (Commonwealth Act No. 146). Key amendments relating to telecommunications are:

- Easing of nationality restrictions: Before the amendatory law, telecommunications and related services were considered public utilities and subject to the nationality restrictions imposed under the Philippine Constitution, Republic Act No. 11659 reclassifies public telecommunications entities as a public service owning 'critical infrastructure,' which the law defines as systems and assets, whether physical or virtual, so vital to the Philippines that the incapacity or destruction of such systems or assets would have a detrimental impact on national security. This amendment allows 100% foreign ownership, subject to reciprocity, national security interest, and in the case of persons and companies engaged in the telecommunications business, obtaining and maintaining International Organization for Standardization (ISO) certifications on information security.
- Exclusion of value-added services (VAS) from the definition of 'telecommunications': A VAS was previously classified as a public telecommunications entity (PTE) and thus subject to the nationality restrictions under the Philippine Constitution.

Republic Act No. 10844 created the Department of Information and Communications Technology (DICT), establishing it as the primary policy-making entity of the government for the national ICT development agenda. Various issuances of the DICT such as Circular No. HRA-003, Circular Nos. 004 and 005, s. 2024, and Circular No. 008, s. 2020, form part of the regulatory framework, setting mandatory guidelines for critical information infrastructure and cybersecurity standards.

Republic Act No. 12234 or the Konektadong Pinoy Act is another key legislation governing telecommunications networks and services. It establishes an open-access framework to improve data transmission connectivity across the country.

Republic Act No. 11934 or the SIM Registration Act is a mandatory law requiring all public telecommunications entities and direct sellers to register the subscriber identity module (SIM) cards of all end-users. This serves

as a vital national measure to establish accountability and curb cybercrimes, text scams, and financial fraud.

Lastly, consumer rights within the sector are protected by Republic Act No. 11202 or the Mobile Number Portability Act, which ensures consumers can keep their existing mobile numbers even if they change their service providers or shift from prepaid to postpaid subscriptions.

12. 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 NTC, which regulates the industry, historically requires providers to secure a certificate of public convenience and necessity (CPCN) or a provisional authority (PA) to operate. Traditionally, securing these authorisations necessitated obtaining a prior legislative franchise from the Philippine Congress.

Now, the applicability of licensing in the Philippines depends on the type of telecommunications service being provided. Generally, the framework is divided into traditional regime for PTEs and a streamlined regime for modern data transmission industry participants (DTIPs).

Under the Public Telecommunications Policy Act, PTEs or entities providing traditional telecommunications services, such as basic telephone services (local exchange operators or those providing basic landline services), international carriers, interexchange carriers (domestic long-distance services), and mobile radio service providers, must undergo a two-tiered authorisation process. First, they must secure a legislative franchise to operate as a public utility or public service. Upon securing this, they are still required to obtain a CPCN or PA from the NTC before commencing operations. Furthermore, if their operations involve the use of the radio frequency spectrum, they must secure separate frequency allocations and radio station licences from the NTC. It must be noted that VAS providers are an exception; they do not require a legislative franchise, but they must still undergo administrative registration process with the NTC.

On the other hand, regulation has recently shifted to encourage broader market participation. Under the Konektadong Pinoy Act, market entry for DTIPs, such as internet service providers and those building data networks, has been streamlined. They are no longer required to secure a legislative franchise or CPCN.

Instead of the traditional franchise requirement, DTIPs can now build, own, and operate network infrastructure (including international gateways, backbone networks, and spectrum resources) through an administrative registration and authorisation process with the NTC. To operationalise this framework, the NTC recently issued Memorandum Circular No. 002-02-2026, which sets out the specific eligibility criteria that applicants must satisfy to register as DTIPs:

- An applicant must be organised and registered under Philippine law, which encompasses sole proprietorships, partnerships, cooperatives, or corporations (including government-owned entities). Lawful forms of foreign presence, such as branch or representative offices, are also legally eligible to operate. For foreign satellite providers, they must establish a local presence and service centre in the Philippines, alongside providing proof of reciprocity from their home country regarding market access.
- Applicants must prove their technical capability by submitting a technical feasibility study, proof of prospective service capacity (e.g., agreements with other DTIPs for bandwidth), and evidence of prospective access to infrastructure. Crucially, applicants are required to have a comprehensive cybersecurity plan in place, with separate guidelines on cybersecurity measures to be issued by the DICT.
- Applicants must prove their financial and economic viability by submitting audited financial statements, economic feasibility studies, and certifications from financial institutions. Applicants must also post a performance bond and maintain a maximum debt-to-asset ratio of 70%. The circular sets strict minimum asset requirements that scale depending on the data transmission segment: PhP 500,000 for last mile providers; PhP 10,000,000 for middle mile providers; PhP100,000,000 for core or backbone network providers; and PhP 1,000,000,000 for international gateway facility providers.

However, there are special circumstances to consider. If a traditional PTE providing basic telephone services also offers data transmission (including internet and digital data), the Konektadong Pinoy Act will apply to them, but only insofar as their data transmission services and the linkage of their networks extended to DTIPs are

concerned. Their traditional basic telephone services (i.e., local exchange telephone service for residence and business establishments provided via the circuit-switched telephone network) are still subject to legislative franchising and CPCN requirements.

Furthermore, passive infrastructure owners, lessors, and operators (such as independent tower companies) are not covered by NTC Memorandum Circular No. 002-02-2026, as their operations are governed separately by DICT guidelines on infrastructure sharing.

13. 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.

Republic Act No. 10175 or the Cybercrime Prevention Act was enacted 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.

The law appoints the National Bureau of Investigation (NBI) and the Philippine National Police (PNP) as the enforcement authorities and regulates their access to computer data. The Office of Cybercrime within the Department of Justice (DOJ) was likewise created and designated as the central authority in all matters related to international mutual assistance and extradition. Further, the law established the Cybercrime Investigation and Coordinating Centre (CICC), an inter-agency body tasked with policy coordination among government agencies and formulation and enforcement of the Philippine cybersecurity plan. The CICC was subsequently attached to the DICT.

The Cybercrime Prevention Act authorises law enforcement authorities, so long as with due cause, to collect or record by technical or electronic means traffic data in real-time associated with specified communications transmitted by means of a computer system. Traffic data that is subject to this authority refers only to the communication's origin, destination, route, time date, size, duration, or type of underlying service. Service providers are compelled to cooperate and assist law enforcement authorities in collection or recording of such information. It bears emphasis that all other data to be collected or seized or disclosed will require a court warrant.

In practice, data access is operationalised by the Philippine Supreme Court through the Rule on Cybercrime Warrants (AM No. 17-11-03-SC). This rule establishes specific warrants: the Warrant to Disclose Computer Data (WDCD), which compels providers to submit subscriber and traffic data; the Warrant to Search, Seize, and Examine Computer Data (WSSECD), which authorises the physical or remote search and seizure of computer systems or storage media containing relevant data; and the Warrant to Intercept Computer Data (WICD), which authorises the real-time collection of communications. The types of data that can be requested encompass basic subscriber information, traffic data (such as communication origin, route, duration, and size), and content data. However, these warrants require a judge to personally determine the existence of probable cause. Furthermore, service providers are bound by strict confidentiality orders regarding the existence of the warrant and the ongoing investigation.

Under the Cybercrime Prevention Act, a service provider is obliged to preserve integrity of traffic data and subscriber information relating to the communication services it provides for a minimum period of six (6) months from the date of the transaction. Content data must be preserved for six (6) months upon receipt of an order from law enforcement authorities. This period may be extended for another six (6) months, although the law specifically provides for instances where the service provider has the obligation to preserve the computer data until the termination of court proceedings.

In addition to the Cybercrime Prevention Act, law enforcement access to communications data is governed by other intersecting legislation such as:

- Republic Act No. 11934 or the SIM Registration Act mandates that all telecommunications end-users must register their SIMs with their service providers, submitting identification details such as their full name and address. The resulting SIM register is deemed absolutely confidential. However, competent authorities, such as cybercrime prevention bodies or prosecutorial offices with subpoena powers, can legally access this data to investigate cybercrimes, text scams, and financial fraud. As a legal safeguard, access

requires the issuance of a subpoena pursuant to an investigation based on a sworn complaint demonstrating that a specific mobile number was used in a malicious or fraudulent act. Alternatively, disclosure may be compelled through a valid court order upon a finding of probable cause.

- Republic Act No. 11930 or the Anti-Online Sexual Abuse or Exploitation of Children (OSAEC) and Anti-Child Sexual Abuse or Exploitation Materials (CSAEM) Act. This law imposes proactive filtering, preservation, and reporting duties on service providers to combat child exploitation. Under Section 9 of the said law, internet service providers (ISPs) and other internet intermediaries are obligated to install available technology, programs, or software to block or filter access to any form of CSAEM. These entities must explicitly prohibit such activities in their terms of service, integrate child protection standards like age-verification and default high-privacy settings, and implement technologies to filter or block illicit content within twenty-four (24) hours of notice. Further, they are obligated to preserve for at least six (6) months subscriber and traffic data, and promptly report suspicious online activities to law enforcement (including PNP and NBI).
- Republic Act No. 11479 or the Anti-Terrorism Act provides specialised mechanisms for the surveillance and interception of communications regarding suspected terrorists. Under Section 16 thereof, law enforcement agents or military personnel are authorised to conduct wiretapping, interception, and the recording of private communications. To execute this, authorities must file an ex parte application and secure a written order from the Court of Appeals upon a finding of probable cause. This judicial order compels service providers to produce customer identification records, call and text data, content, and internet metadata. The surveillance authorisation is limited to an initial period of sixty (60) days, which may be extended by up to thirty (30) days. However, the law prohibits the surveillance of privileged communications, such as those between lawyers and clients, doctors and patients, journalists and their sources, and confidential business correspondence.
- Republic Act No. 10173 or the Data Privacy Act provides for specific data privacy exemptions applicable to law enforcement investigations. Under Section 19 of the law, rights of data subjects are not applicable to processing of personal information gathered for the purpose of investigations in relation to any criminal, administrative or tax liabilities of a data subject. Consequently, when law enforcement agencies collect or compel the production of communications data for legitimate investigations, they are exempt from securing the prior consent of the data subject. However, this exemption is not absolute; the collection and processing of such data must still adhere to the fundamental privacy principles of transparency, legitimate purpose, and proportionality.

14. Telecommunications – Please summarise the principal laws (present or impending) that impose cyber security and/or operational resiliency obligations applicable to the operation of telecommunications infrastructure and/or provision of telecommunications services.

Republic Act No. 10844 or the Department of Information and Communications Technology Act of 2015 (DICT Act) attached the CICC to the DICT and transferred all powers and functions related to cybersecurity to the latter. DICT leads the national effort and implements the National Cybersecurity Plan 2023-2028. Further, while the Philippines does not have a cybersecurity law, the DICT, in the exercise of its mandate under the DICT Act, sets the regulations and policies, including those specifying obligations relating to cyber security and or operational resiliency.

The National Cybersecurity Plan, which classifies telecommunications networks as Critical Information Infrastructure (CII), was recently adopted by Executive Order No. 24, s. 2024. To ensure operational resiliency, private sector enterprises classified as CII shall be required to form their own cybersecurity teams (CERT) and shall coordinate regularly with the DICT. Once an enterprise is officially designated as a CII and notified by the National Cybersecurity Inter-Agency Committee (NCIAC), it must undergo a mandatory onboarding and compliance process within 24 months.

Under DICT Circular No. HRA-003 and related regulatory issuances including DICT Department Circular No. 005, series of 2024, telecommunications companies must maintain comprehensive cybersecurity compliance documentation. They must maintain comprehensive and

audit-ready cybersecurity compliance documentation and implement standardised governance frameworks (such as ISO/IEC guidelines). Furthermore, they are strictly required to conduct formal annual security and vulnerability assessments to evaluate the effectiveness of their security controls. Crucially, they are mandated to report severe or critical cyber incidents (including data breaches, ransomware attacks, and service disruptions) to the National Computer Emergency Response Team (CERT-PH) within 24 hours of detection.

Furthermore, the Konektadong Pinoy Act mandates the reporting of material cybersecurity incidents that disrupt network operations. DTIPs are mandated to report material cybersecurity incidents that disrupt network operations or compromise the integrity, confidentiality, or availability of transmitted data. Under its implementing rules and regulations, these entities must also adhere to national and global cybersecurity standards. To ensure long-term operational resiliency, DTIPs are required, within two (2) years of their initial registration, to secure a formal cybersecurity certification from a recognised third-party organisation based on standards benchmarked by the DICT.

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?

The development of technical standards for mobile communications and emerging connected technologies is governed by a combination of national regulatory bodies, local organisations, and the adoption of frameworks from international SSOs.

The NTC references and adopts standards set by international bodies, particularly the International Telecommunication Union (ITU) for spectrum management and mobile communications, and the Institute of Electrical and Electronics Engineers (IEEE) for wireless local networks.

The DICT and National Privacy Commission (NPC) frequently reference International Organization for Standardization (ISO) standards. For instance, the NPC uses ISO/IEC frameworks (such as ISO 27001 and 27701) as benchmarks for privacy and information security management systems in its regulatory issuances, while the DICT mandates ISO compliance for CII.

International SSOs frequently adopted in the Philippines include, as mentioned, the ITU (for radio frequency allocation and mobile telecommunications networks), the IEEE (for wireless communications, networking, and hardware engineering), and the ISO and IEC (foundational technical specifications for data security, digital health systems, and connected infrastructure). Also, the Internet Engineering Task Force (IETF) and Electronic Industries Alliance (EIA) provide critical standards for internet architecture, protocols, and electronic hardware interoperability.

Local professional organisations like the Institute of Integrated Electrical Engineers of the Philippines (IIEE) or the Institute of Electronics Engineers of the Philippines (IECEP) also contribute expertise to the formulation, review, and adoption of local electrical and engineering standards relevant to connected devices and their supporting infrastructure.

For newer connected technologies, standard setting is still in its early stages, but the Bureau of Philippine Standards (BPS) is legally mandated to develop, promulgate, and implement Philippine National Standards (PNS) for various products, systems, and technologies. The BPS, as well as other relevant agencies like the Land Transportation Office (LTO), Department of Transportation (DOTr), and Department of Health (DOH), frequently adopt or harmonise international standards (such as those from ISO, IEC, and ITU) into local PNS or their respective frameworks.

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

Technical standards ensure that devices from different manufacturers can communicate seamlessly on shared networks. Establishing common technical baselines (such as universal IEEE or IETF protocols) encourages a competitive market ecosystem where new innovators and service providers can easily integrate and scale their solutions. This interoperability prevents market fragmentation, lowers costs for consumers, and may accelerate the development and deployment of newer connected technologies, such as digital health tools and autonomous vehicles.

17. Data Protection – Please summarise the

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

The principal statute is Republic Act No. 10173, or the Data Privacy Act of 2012, together with its implementing rules and the circulars and advisories issued by the NPC. The Data Privacy Act of 2012 is the Philippines' omnibus data protection law. It regulates the processing of personal information by natural and juridical persons, including PICs and PIPs, and may apply to processing outside the Philippines where the statutory connecting factors to the Philippines are present.

The Data Privacy Act of 2012 requires processing to observe transparency, legitimate purpose and proportionality, and to have an applicable lawful basis. More restrictive conditions apply to sensitive personal information and privileged information. It also gives data subjects rights to information, access, correction, objection or blocking in appropriate cases, erasure or destruction, damages and data portability.

PICs are required to implement reasonable and appropriate organisational, physical and technical security measures, remain accountable for personal data outsourced or transferred domestically or internationally, and use contractual or other reasonable means to provide a comparable level of protection.

A notifiable personal data breach must generally be reported by the PIC to the NPC and affected data subjects within 72 hours after knowledge of, or reasonable belief in, the occurrence of the breach.

The NPC administers and enforces the Data Privacy Act of 2012. Its more recent issuances address, among other matters, registration and notification requirements, administrative fines, security of personal data, legitimate interest, consent, model contractual clauses for cross-border transfers, artificial intelligence systems that process personal data, privacy engineering throughout the systems life cycle and the scraping of publicly available personal data. Sector-specific statutes and regulations may impose additional confidentiality, cybersecurity, consumer-protection or record-retention obligations.

For government data, additional rules supplement the Data Privacy Act of 2012. The E-Governance Act institutionalises the government's transition to an integrated digital government. Among other matters, it requires e-government programmes and systems to comply with applicable data privacy and security standards, requires a mandatory privacy impact assessment for proposed systems for processing personal data included in the E-Government Master Plan, mandates minimum information security standards, and requires government agencies to adopt Privacy-by-Design, Privacy Engineering and Privacy-by-Default in systems, processes, software applications and services that process personal data.

Executive Order No. 119, series of 2026, entitled Updating the Government Data Classification, Establishing a Data Residency Framework, and for Other Purposes (Executive Order No. 119, series of 2026), further updates the government data classification framework and establishes rules on data residency, cross-border transfers and information security. It principally covers government data in digital or hybrid form which is owned, processed or controlled by covered government agencies and instrumentalities. It does not apply to private-sector or commercial data owned by private entities, but it applies to government data or information processed or stored by private entities on behalf of a government agency. Government agencies which procure or use cloud service providers or other private entities for the storage or processing of government data remain responsible for data security and must ensure that appropriate contractual and technical safeguards are included in their arrangements.

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 Data Privacy Act of 2012 prescribes criminal penalties which are imposed by the courts. The NPC may recommend criminal prosecution to the DOJ but may not itself impose these criminal penalties.

Under the Data Privacy Act of 2012, a combination or series of acts defined in Sections 25 to 32 thereof, which cover unauthorized processing of personal information and sensitive personal information, accessing personal data due to negligence, improper disposal of personal data, processing of personal data for unauthorized purposes, unauthorized access or intentional breach, concealment of security breaches involving sensitive personal information, malicious disclosure or unauthorized disclosure, is punishable by imprisonment of three (3) to six (6) years and a fine of PhP 1 million to PhP 5 million. The longest term of imprisonment prescribed for a standalone offence is seven (7) years, which applies to the processing of sensitive personal information for unauthorised purposes. Where the

personal information of at least 100 persons is harmed, affected or involved, the maximum penalty within the statutory range applicable to the offence must be imposed.

Under NPC Circular No. 2022-01, the NPC also imposes administrative fines based on its categorisation of infractions. Most fines are computed based on a percentage of the offender's annual gross income for the preceding year; however, the maximum administrative fine is set at PhP 5 million for a single act of processing by a PIC or PIP, whether that act gives rise to one or several infractions. The PhP 5 million ceiling applies regardless of whether the percentage-based computation would otherwise result in a higher amount. The ceiling applies per processing act; separate processing acts may be assessed separately.

Subject to the PhP 5 million cap for a single processing act, the administrative fines are set at:

- For grave infractions: from 0.5% to 3% of the offender's annual gross income for the immediately preceding year in which the infraction occurred. These include violations of the general privacy principles or data-subject rights affecting at least 1,001 data subjects, and the repetition of an infraction previously penalised under the circular.
- For major infractions: from 0.25% to 2% of the offender's annual gross income for the immediately preceding year in which the infraction occurred. These include violations of the general privacy principles or data-subject rights affecting between one and 1,000 data subjects, failures to implement or require appropriate security measures, and failures to make the required personal data breach notifications, unless the conduct is punishable under section 30 of the Data Privacy Act of 2012.
- For other Infractions concerning registration or updating of information: from PhP 50,000 to PhP 200,000.
- Failure to comply with an NPC order, resolution or decision: up to PhP 50,000, in addition to the fine imposed for the original infraction.

The NPC may also issue compliance or enforcement orders, award indemnity, issue cease-and-desist orders and impose a temporary or permanent ban on processing where the statutory and procedural requirements are satisfied.

Executive Order No. 119, series of 2026, the recent regulation covering government data (in contrast with private sector or commercial data owned by private entities), does not fix any administrative fine in addition to those specified under the NPC framework. Instead, section 14 thereof states that failure by an erring public official or employee to comply constitutes a ground for administrative or disciplinary sanctions under existing laws and regulations, without prejudice to criminal, civil or other liabilities.

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

Technology contracts in the Philippines typically include clauses on data processing, implementation of security measures, and protocols for breach notification to comply with the Data Privacy Act of 2012. These contracts, which involve personal data, should first allocate the parties' roles under the Data Privacy Act of 2012.

Where a PIC engages a PIP, the arrangement must be governed by a binding contract or other legal act. The contract must state the subject matter and duration of processing, its nature and purpose, the types of personal data and categories of data subjects, the controller's rights and obligations, and the geographic location of processing.

The contract should also require the processor to act only on documented instructions; preserve confidentiality; implement appropriate security measures; obtain prior authority before appointing another processor and flow down equivalent obligations; assist with data-subject requests, security and regulatory compliance; return or delete personal data at the end of the services; make information available for audits and inspections; and notify the controller if an instruction would breach Philippine data protection laws. In practice, technology contracts also deal expressly with incident escalation, breach notification, retention, deletion, business continuity, audit rights, data localisation where sector rules require it, international transfers and allocation of responsibility for regulatory investigations and claims. For cross-border processing, the controller remains accountable and must use contractual or other reasonable means to maintain a comparable level of protection. The NPC's model contractual clauses for cross-border transfers may be adopted or adapted for

this purpose.

Additional requirements apply where a technology contract involves Philippine government data or government information systems.

Under Section 2 of Executive Order No. 119, series of 2026, a government agency which procures or uses a cloud service provider or other private entity for the storage or processing of government data remains responsible for ensuring data security and compliance and must ensure that appropriate contractual and technical safeguards are included to protect the data handled by the service provider.

If contracted to process or store government data or information on behalf of a government agency, private entities, including those engaged in public-private partnerships, public services, public utilities, critical infrastructure or in strategic or sensitive subjects, must also comply with the requirements of Executive Order No. 119, series of 2026. This obligation is limited to government data and information, while other data they process or store, including private sector or commercial data owned by private entities, are not covered.

The E-Governance Act provides a further government-sector layer. Government agencies are responsible for information security protections commensurate with the risk and magnitude of harm for information and systems used or operated by the agency, its contractor or another organisation on its behalf. The E-Governance Act also requires Privacy-by-Design, Privacy Engineering and Privacy-by-Default in systems and services processing personal data and permits government contracts and partnerships with the private sector subject to laws and rules on public accountability, transparency and good governance. Proposed systems for processing personal data included in the E-Government Master Plan are also subject to a mandatory privacy impact assessment, and E-Government systems are subject to minimum information-security standards prescribed by the Department of Information and Communications Technology.

Given the global nature of technology services, commercial contracts may reference external data protection regimes, such as the EU GDPR, as a baseline standard for vendor compliance, even if the contract has no clear international element.

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

The Philippines does not have a comprehensive cybersecurity law. However, there are existing laws, most of which are penal in nature, that deal with acts that may interfere with computer and IT systems and their security.

The Cybercrime Prevention Act protects the integrity of computer and communications systems, networks, and databases, as well as the confidentiality, integrity, and availability of computer data and declares the following offenses as cybercrimes:

- offences against the confidentiality, integrity and availability of computer data and systems (illegal access, illegal interception, data interference, system interference, misuse of devices, and cybersquatting);
- computer-related offences (computer-related forgery, computer-related fraud, and computer-related identity theft); and
- content-related offences (cybersex, child pornography, unsolicited commercial communications, and cyber libel).

In addition, the National Cybersecurity Plan 2023-2028 serves as the strategic policy framework designed to ensure a secure, trusted, and reliable national cyberspace.

Republic Act No. 8792 or the Electronic Commerce Act of 2000 penalises the following acts:

- hacking or cracking, or any access in order to corrupt, alter, steal, or destroy using a computer or other similar device without the knowledge and consent of the owner
- piracy
- violations of consumer laws through transactions covered by or using electronic data messages or documents

Sector-specific regulations also govern cybersecurity. For example, the BSP recently issued Memorandum No. M-2026-034, which directs BSP-supervised institutions to manage the cybersecurity risks associated with frontier AI systems. The memorandum encourages the financial sector to adopt AI-enabled defensive measures, enforce hardware-backed multi-factor authentication, and implement robust AI governance frameworks to counter adaptive cyber threats.

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?

Under the Cybercrime Prevention Act, offences committed against critical infrastructure carry a maximum penalty of reclusion temporal (12 to 20 years imprisonment) or a fine commensurate to the damage incurred, or both.

22. Cybersecurity – Are there any cybersecurity regulatory frameworks in your jurisdiction which require registration for certain sectors or services?

There are two (2) main cybersecurity legal frameworks currently in place. The principal laws behind these frameworks are the Data Privacy Act of 2012 and the Cybercrime Prevention Act, which focus on data protection and cybercrime enforcement, respectively. The NPC leads the data protection framework, while the DICT and law enforcement agencies implement the cybercrime framework.

The cornerstone of privacy protection in the Philippines, the Data Privacy Act of 2012 requires covered PICs and PIPs to register their data protection officers and data processing systems. Aside from requiring the implementation of technical, organizational, and physical controls to ensure data integrity, confidentiality and availability, compliance with requirements relating to breach reporting and annual security incident reporting is also mandatory.

On the other hand, the Cybercrime Prevention Act addresses instances of criminal digital activity and provides the regulatory framework for digital investigation and forensics, preservation of evidence and law enforcement.activity, including cooperation among government agencies. The DICT, as the primary government agency for cybersecurity, accredits cybersecurity firms under the DICT Trusted Assessment Provider (DTAP) program. Once accredited, firms are listed in the DICT registry and are then authorised to provide services and conduct formal cybersecurity assessments for public and private sector clients. Under Department Circular No. HRA-03, the DICT also formalised the framework for cybersecurity posture assessment laboratory accreditation.

23. Cybersecurity – Please summarise the regulatory framework for the reporting of cybersecurity incidents.

The regulatory framework for reporting cybersecurity and data incidents depends on the nature of the breach and the affected entity.

For the NPC, Personal Data Breach Notification Forms (PDBNFs) should be accomplished and submitted within seventy-two (72) hours upon knowledge of or reasonable belief by the personal information controller (PIC) or personal information processor (PIP) that a personal data breach has occurred. Notably, under pertinent NPC guidelines (Circular No. 16-03 and Advisory No. 18-02), the framework not only covers notice to NPC, but also mandates the direct notification of the affected data subjects within the same 72-hour timeframe. Notification to data subjects is required when the breach involves sensitive personal information or data that could be used to enable identity fraud, and there is a reasonable belief that the unauthorised acquisition is likely to give rise to a real risk of serious harm to the affected individuals. In general, the notice contains the nature of the breach, sensitive personal information possibly involved, measures taken by the entity to address the breach, and details of contact person for more information.

On the other hand, for the DICT and pursuant to DICT Department Circular No. 005 s. 2024, all government agencies and Critical Information Infrastructures (CIIs) are required to report cybersecurity incidents (e.g., data breaches, ransomware, unauthorized access) to CERT within 24 hours of detection.

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

There is no specific regulator of artificial intelligence in the Philippines. However, general data privacy laws that apply broadly to AI are implemented and enforced by the NPC.

Meanwhile, there are regulations on the use of AI that are sector-specific, and these are implemented by the relevant government body that issued them. These regulations typically deal with the use of AI within these sectors and are not to be applied to firms, entities or individuals outside these sectors.

Interestingly, there are pending industry-agnostic legislations in the Philippine Congress that seek to regulate AI, and some of them propose to create a bureau

or council that will oversee its implementation.

While there are no bodies providing regulatory oversight over AI use, there is a handful of public institutions dedicated to AI research and development, and building the country's national AI strategy, including the National Artificial Intelligence Centre for Research and Innovation under the Department of Science and Technology, Centre for AI Research under the Department of Trade and Industry (DTI), and the Education Centre for AI Research under the Department of Education.

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

There is no specific law or regime that governs the deployment and use of AI. Currently, several regulators have made it their mission to regulate AI through sector-specific guidelines and principles, with the exception of the NPC which has broader authority since its mandate transcends industries, to the extent personal data is concerned.

The NPC expressly PICs and PIPs to adhere to general data privacy principles, including determining the correct lawful basis for the processing and upholding data subject rights, if their processing systems involve the use of AI (NPC Advisory No. 2024-04). Noteworthy from this issuance is the NPC's move to require PICs and PIPs to institute governance mechanisms to ensure 'responsible and ethical processing of personal data' when AI systems are developed and deployed. Such mechanisms include the conduct of privacy impact assessments, implementation of common industry security standards and most notably, the creation of a dedicated AI ethics board and intervention of humans in decision-making and review of outputs of AI systems. The regulation also empowers data subjects to contest automated decisions affecting their rights and freedoms. Further, the use of automated personal data processing where decisions are made involving a data subject, and are totally independent of human intervention, must be registered to the NPC following the procedure in NPC Circular No. 2022-04. These systems often involve profiling.

Meanwhile, the use of AI in the government is regulated by the Principles for the Ethical and Responsible Development, Deployment, and Use of Artificial Intelligence (AI) in the Government, a joint circular from the DICT and the Civil Service Commission (CSC). The circular highlights that the use of AI must adhere to several foundational principles, culled from various international practices and guidelines, such as human-centricity, transparency and explainability, fairness and non-discrimination, among others. Within the judiciary, the Supreme Court of the Philippines enforced the Governance Framework on the Use of the Human-Centred Augmented Intelligence in the Judiciary for the use of AI by judges and court personnel.

In the financial services sector, the BSP, the Philippine central banking authority, recently issued the Governance Principles for Artificial Intelligence (AI) in Financial Services, which highlights the ethical and responsible use of AI by adhering to the principles of sustainability, transparency, accountability, responsibility and security (or what the BSP calls the STARS principles). Entities under the BSP's jurisdiction are also called to put their AI systems into various checkpoints within its lifecycle to ensure risks are mitigated or controlled in every opportunity. Ultimately, the BSP recommends that financial institutions develop their respective AI Governance Frameworks following the guidelines and principles.

Additionally, the BSP issued Recommendations for Managing Emerging Risks Arising from Frontier Artificial Intelligence Systems, which outlines specific recommendations to combat known and emerging risks from a cybersecurity perspective.

Among dozens of pending bills, the standouts are the following:

- House Bill No. 10362, filed in July 2026, seeks to establish the AI Bill of Rights in favour of persons affected by AI systems or automated decision-making, including the right to transparency, right to information, right against discriminatory automated decisions, right to human review, right to data privacy and data protection, right to be forgotten, right to safety and right to disclosure of synthetic data. It also intends to impose obligations on employers deploying high-impact AI systems that may substantially affect the core functions of their workforce, including six-month advance notice before deployment.
- Senate Bill No. 2097, filed in May 2026, focuses on regulating the use, development and deployment of AI in the essential services (e.g., healthcare delivery, public education and emergency response), critical infrastructure (e.g., transportation systems, financial infrastructures and telecommunications),

media, and research and development. The bill adopts the risk-based approach of several international legislations by categorising AI systems into low risk, medium risk and high risk, where each category is subject to varying compliance requirements, including registration of high-risk AI systems with the Philippine AI Regulation Council, which the bill seeks to establish.

- House Bill No. 9601, seeks to establish the Artificial Intelligence Development Authority that is tasked to oversee the development and deployment of AI technologies and ensure compliance with AI ethics principles and guidelines. The bill seems to be innovation-friendly compared to other bills.
- Senate Bill No. 182 plans to create the National Task Force on Digital Economy Job Disruption whose mandate is to identify industries at high risk of AI or digital disruption and evaluate its impact on workers. The task force's findings will feed into policies to protect workers' rights.

26. 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 is no specific law or regime in respect of the deployment and use of large language models (LLMs) and generative AI (including agentic AI).

Nonetheless, the above-cited sector-specific guidelines and regulations may apply broadly. For instance, BSP's Governance Principles for Artificial Intelligence (AI) in Financial Services applies to AI systems, which, it clarifies, may operate 'with varying levels of autonomy', citing generative AI and agentic AI as covered in the definition.

With respect to penal provisions, House Bill No. 2319 expressly criminalises child sexual abuse or exploitation material generated through the use of AI, as well as its distribution (i.e., sharing or reposting in social media will be penalised) and sale. Under the same bill, private sectors, such as internet intermediaries, are given obligations to ensure the creation, production, distribution and sale of such AI-generated materials are immediately taken down or access thereto is blocked.

27. 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?

There is no specific law that requires or recommends technology contracts to include provisions that deal with AI risk.

In case the personal data processing is outsourced, the implementing rules and regulations of the Data Privacy Act of 2012 require that the relationship between PICs and PIPs be governed by a contract, which must contain the provisions set out in Section 44(b) of the implementing rules and regulations. The required stipulations obligate PICs and their PIPs to implement appropriate security measures and comply with the data privacy law, regulations and other issuances of the NPC. As shown in NPC Advisory No. 2024-04, PICs and PIPs are mandated to institute appropriate and effective governance mechanisms. They are also tasked with creating additional safeguards to ensure protection against the significant risks to the rights and freedoms of data subjects arising from the use of AI, and such mechanisms shall allow for meaningful human intervention.

28. 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?

We find that it is typical to contain protections and prohibitions against unauthorised use of intellectual properties or copyrighted works through training and fine-tuning systems, but it is not common to stipulate on ownership of outputs or AI-generated content.

Interestingly, among the pending bills in the Philippine Congress, Senate Bill No. 2097 seeks to prohibit the use of 'original works' as defined in IP Code for training and fine-tuning AI systems and for generating content that substantially reproduces such works, without authorization from the rights holders.

29. 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?

There is no specific law or regulation that governs the use of blockchain.

Nonetheless, we see a surge of initiatives that allow for widespread adoption of blockchain in the public sector. For instance, under the E-Governance Act, government bodies covered in the law are mandated to install a Chief Information Officer, and one of her functions is to accelerate the use of blockchain.

In the Congress floor, Senate Bill No. 1330 seeks to establish a blockchain-based budget system where all records of the national budget are to be recorded as digital public assets. The bill was borne out of the recent allegations of misappropriation among public officials. The bill mandates that all records of the national budget, from preparation, legislation, execution and audit, must be recorded in the blockchain. The system must also provide real-time access to allow independent verification by interested stakeholders, including the public itself.

With respect to digital assets, the most prominent regulations come from the BSP and the Securities and Exchange Commission (SEC):

- The SEC Guidelines on the Operations of Crypto-Asset Service Providers and The SEC Rules on Crypto-Asset Service Providers, which outline the registration and licensing regime for crypto-asset service providers (CASPs) and the rights of their consumers. The regulations specifically acknowledge that these assets may take the form of investments when made available to the public, and as such, the SEC would regulate these assets the same way it does for securities (which can be seen from the similarities between the requirements, such as disclosure and registration statements). The SEC's regulation is seen from the perspective of financial consumer protection, market conduct and establishment of a corporate entity.
- The Manual of Regulations for Non-Bank Financial Institutions by the BSP, on the other hand, is more concerned about regulating virtual asset service providers (VASPs), or those that engage in activities that provide facility for the transfer or exchange of virtual assets, such as exchange between virtual assets and fiat currencies, transfer of virtual assets, exchange between one or more virtual assets, and safekeeping and/or administration of virtual assets.

The two regulators define crypto-asset and virtual asset as digital representations of value, relying on secured decentralized ledger, which can be traded, transferred or stored electronically. However, the SEC seems to regulate only crypto-assets that satisfy the definition of investments, while the BSP recognizes that virtual assets can be used for payment purposes, except the payment of virtual goods and services within an online game are not considered virtual assets (e.g., gaming tokens).

A bill pending before the Senate (Senate Bill No. 433) seeks to define 'digital assets' as e-money (representation of fiat currency backed by an equivalent fiat currency) and virtual assets. Additionally, the bill wants to clarify the lead agency or regulator of each type: SEC for virtual assets and BSP for e-money. House Bill No. 4792, on the other hand, seeks to recognize real-world asset tokenization to allow digital representation of ownership rights or claims in assets using blockchain tokens. The eligible assets include Philippine-registered corporations, real estate, commodities, intellectual properties, securities, and public-private partnership projects. The bill also goes far as to authorize the secondary trading of these tokenized assets.

30. 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 is no principal law or regulation governing search engines as a distinct class of online service, although legal obligations may arise under special laws depending on the functions they perform and the content or transactions involved. For example, search engines and portals are expressly included within the definition of 'internet intermediaries' under Republic Act No. 11930 or the Anti-Online Sexual Abuse or Exploitation of Children and Anti-Child Sexual Abuse or Exploitation Materials Act (OSAEC and CSAEM Act). They are consequently subject to applicable duties concerning data preservation, blocking and takedown, reporting, disclosure pursuant to lawful process and the adoption of mechanisms to prevent, detect and respond to online sexual abuse or exploitation of children and child sexual abuse or exploitation materials.

The regulation of marketplaces other digital platforms similarly depends on the functions they perform, including whether such facilitate e-commerce, process personal data, host or index unlawful content, infringe intellectual property rights or engage in conduct affecting competition. This functional approach is also relevant to search engines. Although search engines are not expressly defined as a separate category under Republic Act No. 11967, or the Internet Transactions Act of 2023 (ITA), particular features operated by a search engine may fall within the ITA where they satisfy the statutory definition of a 'digital platform' or 'e-marketplace' and are used for a covered internet transaction.

Online marketplaces used for covered e-commerce transactions are principally governed by the ITA and its implementing rules. The ITA applies to business-to-business and business-to-consumer internet transactions within the mandate of the DTI where at least one party is situated in the Philippines, or where the digital platform, e-retailer or online merchant avails itself of the Philippine market and has minimum contacts in the country. Consumer-to-consumer transactions and online media content are excluded from its scope.

The ITA defines a 'digital platform' as an information and communications technology-enabled mechanism which connects and integrates producers and users in an online environment where goods and services are requested, developed and sold, and data is generated and exchanged. An 'e-marketplace' is a digital platform whose business is to connect online consumers with online merchants, facilitate shipment, logistics or post-purchase support, and otherwise retain oversight over the consummation of the transaction. Other digital platforms may also be subject to the ITA where they are used to conduct e-commerce but do not retain oversight over the consummation of the transaction.

Accordingly, a search engine is not subject to the ITA solely because it crawls, indexes, retrieves or ranks online content. Those activities, without more, do not necessarily constitute the connection of producers and users in an environment where goods or services are requested, developed or sold, or the facilitation of an internet transaction. However, where a search engine also displays merchant product offers, connects consumers with online merchants or provides other commercial features through which covered business-to-business or business-to-consumer transactions are facilitated, those functions may bring it within the ITA as a digital platform. If it also performs the functions specified for an e-marketplace and retains oversight over the consummation of the transaction, it may be regulated as an e-marketplace. Its classification therefore depends on its actual commercial functionality rather than its description as a search engine.

In addition, the Electronic Commerce Act of 2000, provides a conditional limitation of liability for a service provider in respect of an electronic data message or electronic document to which it merely provides access. The protection applies only where the provider lacks actual knowledge or awareness of apparent unlawfulness, does not knowingly receive a financial benefit directly attributable to the unlawful activity and does not directly commit, induce or cause the unlawful act. It expressly leaves unaffected obligations arising from contract, licensing or regulatory regimes, written law and court-ordered injunctive relief. Accordingly, it cannot be relied upon to avoid the specific duties imposed by the ITA or other statutes.

Depending on their activities, search engines and marketplaces are also subject to:

- the Data Privacy Act of 2012, in relation to personal data processing;
- the Consumer Act of the Philippines, as amended, in relation to consumer protection;
- Republic Act No. 8293, or the IP Code, in relation to intellectual property infringement; and
- Republic Act No. 10667, or the Philippine Competition Act, in relation to anti-competitive agreements, abuse of dominance and merger control, especially considering that the implementing rules of the ITA expressly require compliance with applicable competition laws.

Republic Act No. 12023, which further amended the National Internal Revenue Code of 1997, also treats online search engines and online marketplaces as digital services for value-added tax purposes. Resident and non-resident digital service providers may be required to assess, collect and remit value-added tax on digital services consumed in the Philippines.

For financial marketplaces, BSP Circular No. 1237, Series of 2026 establishes a sector-specific framework for BSFIs which operate or participate in digital financial marketplaces or present financial products through other digital platforms. The framework is intended to support responsible innovation while imposing governance, risk-management, consumer-protection and data-governance requirements on covered institutions.

31. 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?

There is no single law or regulation that governs social media and online platforms. Social media and online platforms are regulated according to their functions, the content concerned and the persons affected. Matters connected with the operation and use of social media and online platforms, such as privacy, cybercrime, defamation and cyber libel, online bullying, photo and video voyeurism, intellectual property, identity theft, and child exploitation are governed by multiple laws.

Where a social media platform is used for e-commerce, the ITA and its implementing rules apply. A social media platform may be treated as an e-marketplace if it retains oversight over the consummation of the transaction; otherwise, it may be regulated as another digital platform. The resulting duties include commercial-account transparency, merchant and product disclosures, controls for regulated goods, redress mechanisms, data protection, ordinary diligence and compliance with the regulations of the Department of Trade and Industry.

The OSAEC and CSAEM Act is the principal statute imposing direct duties on internet intermediaries for child online safety. 'Internet intermediaries' expressly include internet service providers, hosting providers and domain registrars, search engines and portals, e-commerce intermediaries, internet payment-system providers and participative network platform providers, including social media intermediaries. This law does not provide a broad immunity from intermediary liability. It instead imposes affirmative statutory duties and criminal sanctions for non-compliance.

Republic Act No. 11313, or the Safe Spaces Act, criminalises gender-based online sexual harassment. It covers conduct using information and communications technology to threaten or intimidate a victim; unwanted sexual, misogynistic, transphobic, homophobic or sexist remarks; cyberstalking and incessant messaging; non-consensual uploading or sharing of sexual content or unauthorised recordings; online impersonation; false statements intended to damage reputation; and false abuse reports used to silence a victim. The Philippine National Police Anti-Cybercrime Group receives complaints and apprehends offenders, with the CICC coordinating measures to monitor and penalise the conduct. It is worth noting that this legislation is principally directed at the perpetrator rather than creating a general intermediary-liability regime.

Other relevant statutes include:

- Republic Act No. 9995, or the Anti-Photo and Video Voyeurism Act of 2009, for the non-consensual recording, copying or distribution of intimate images;
- the Cybercrime Prevention Act of 2012, for offences such as illegal access, computer-related identity theft and cyber libel;
- the Data Privacy Act of 2012 for unlawful processing or disclosure of personal data; Republic Act No. 10627,
- the Anti-Bullying Act of 2013, for cyberbullying in basic education; and
- Republic Act No. 11862, or the Expanded Anti-Trafficking in Persons Act of 2022, for instances where online platforms are used to recruit, facilitate or exploit victims.

32. 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?

There is no single regulatory maximum sanction because Philippine online-safety obligations are distributed across several statutes, and the most serious sanctions are criminal penalties imposed by the courts rather than administrative fines imposed by a regulator.

For breach of the private-sector duties under the OSAEC and CSAEM Act, the first offense carries imprisonment and a fine of PhP 1.2 million to PhP 2 million. A subsequent offense carries a fine of PhP 2 million to PhP 3 million, revocation of the license or franchise to operate and immediate closure where applicable. If the offender is a juridical person, the responsible owner, manager, partner, director or officer may be liable; the corporation may also be fined 10% to 30% of its net worth and its licence or permit may be revoked.

For the substantive offences under the OSAEC and CSAEM Act, the highest prescribed sanction is life imprisonment and a fine of PhP 5 million to PhP 20 million for a syndicated or large-scale violation.

Under the Safe Spaces Act, gender-based online sexual harassment is punishable also by imprisonment, a fine of PhP 100,000 to PhP 500,000, or both; where the perpetrator is a juridical person, its licence or franchise is automatically revoked. These are judicially imposed criminal sanctions.

Regulatory measures under the ITA, where the unsafe online conduct also concerns e-commerce, may additionally include compliance, takedown and blacklist orders and administrative fines.

33. 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 is no specific law or regulation that governs spatial computing, augmented reality, extended reality, virtual reality and the 'metaverse.'

It is interesting to note that Philippine Creative Industries Act recognizes that virtual, augmented or mixed reality games are part of the creative industries under the 'digital interactive media domain.' This means that industry players and workers within this domain are required to have a representation in the Philippine Creative Industries Development Council, tasked with formulating and implementing the Philippine Creative Industries Development Plan, assisting in the protection of intellectual property rights of the Filipino creative industry stakeholders, among others.

34. 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 is no specific law or regulation (present or impending) that governs quantum computing.

Interestingly, the National Internal Revenue Code, as amended by the Corporate Recovery and Tax Incentives for Enterprises Act, and the 2026 Strategic Investment Priority Plan offer fiscal incentives to enterprises engaged in developing innovation related to quantum computing.

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

There is no specific law or regulation that applies to data centres, but existing laws on data privacy, cybersecurity, foreign investment restrictions, land ownership, environmental impact, energy and water, are to be applied to the operations of data centres.

Nonetheless, if a data centre will offer 'enhanced services', such as audio-conferencing services, audio and video conferencing services, virtual private network service and hosting services, it will qualify as a VAS provider under the regulation of the NTC. It must then apply for a Certificate of Registration from the NTC, which has a validity of five (5) years. If a data centre operator provides data transmission services (or the process of sending and receiving digital or digitised analogue signals over a communication medium one (1) or more computing networks, communication or electronic devices), then it may be considered DTIP subject to a separate registration regime of the NTC under the Konektadong Pinoy Act. The specific regulations that may be applicable to data centres would therefore depend on their additional services.

Further, data centres contracting with public entities must keep in mind the data classification framework, data sovereignty and data residency rules provided in DICT's Prescribing the Philippine Government's Cloud First Policy, as amended, and further amended by the Office of the President in Executive Order No. 119, series of 2026. Depending on the classification of the government data, the data must be stored within the Philippine territory, restricted to an on-premise infrastructure or may be stored outside the Philippine jurisdiction.

House Bill No. 5169 seeks to create at least one (1) public data centre network in every province in the Philippines, to be regulated by the DICT, which should provide services to local government units, state universities and colleges and private entities through open access rules and standard contracts with DICT. Meanwhile, House Bill No. 10362 intends to obligate data centre operators, among others, to conduct meaningful and timely consultations with communities that may be displaced or whose resources may be affected by the operation of data centres, and to disclose information on their annual energy and water consumption and sustainability measures.

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

1. There will be a climate- and sustainability-focused shift in the regulation of AI and the infrastructures that power it. More technology investments enter the country amidst the background of the worsening climate. As it becomes clearer that these investments and

infrastructures strain energy sources and cause various types of pollution, we predict that more communities and advocacy groups will band together to clamour for legislation that will provide protection, create direct accountability and responsibility, and address existing and emerging risks.

2. Whether through an omnibus statute or coordinated rules issued by the NPC, the BSP, the DICT and other sector regulators, future regulation is likely to impose obligations on developers, providers and deployers of AI systems in proportion to the risks those systems present. These obligations may include classifying AI systems according to risk, conducting impact assessments before and during deployment, documenting the source and quality of training data, informing affected persons when AI is used, maintaining appropriate human oversight and audit trails, implementing cybersecurity safeguards, assigning responsibility for automated decisions, and labelling or restricting deceptive synthetic media. The common purpose will likely be geared toward addressing the opacity of AI systems and the difficulty of identifying responsibility when their use results in discrimination, misuse of personal data, security breaches or deceptive content, among others. This direction is already visible in the National Artificial Intelligence Strategy Roadmap 2.0, the NPC's guidance for AI systems processing personal data, and the Supreme Court's 2026 governance framework for human-centred augmented intelligence.

3. Modernization of the IP Code. It is likely that the IP laws of the Philippines will be amended to include rules for emerging technologies such as blockchain and AI.

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

We do not see provisions addressing sustainability / net-zero obligations or similar environmental commitment as a common practice in technology contracts. Rarely, these commitments can be seen in the public-facing platforms of technology vendors, which can be taken as them shying away from giving their customers power to enforce such commitments contractually. However, public companies and multinational enterprises, which may be subject of sustainability reporting or similar obligations under existing regulations or corporate policies, may require stipulation of such commitments with their technology vendors.

If the technology contracts are with government entities, vendors should consider that procuring entities are mandated to implement a sustainable public procurement program under the New Government Procurement Act, which may impact their contractual obligations.

Contributors

Maria Pia A. Urgello
Senior Partner
piaurgello@val.law

Mary Aubbrey B. Lim-Barreras
Senior Partner
aubbreylim@val.law

Reeneth B. Santos
Junior Partner
reenethsantos@val.law

Mitchel Q. Tuazon
Junior Partner
mitchel.q.tuazon@val.law

Anna Rochelle D. Payongayong
Junior Associate
annapayongayong@val.law

Lesley Ysabel B. Sumagpang
Junior Associate
lesleysumagpang@val.law