Indonesia

Fahrul S Yusuf and Mohammad K Bratawijaya
SSEK Legal Consultants

General

1 How can the government's attitude and approach to internet issues best be described?

The Indonesian government initially adopted a conservative and relatively traditional approach to regulating internet-based activities. Prior to 2008, there was no legislation or guidelines in Indonesia that regulated the internet or how electronic information was offered and consumed, for both commercial and non-commercial purposes. In the five to seven years before 2008, Indonesia experienced the rapid development of information technology and the number of internet users in the country soared as the internet became the most popular medium to access electronic information. In response to this growth, the Indonesian government issued an underlying regulation to address potential issues resulting from activities conducted on the internet. On 21 April 2008, through the House of Representatives, the Indonesian government issued Law No. 11 of 2008 on Electronic Information and Transactions (the ITE Law).

The idea behind the ITE Law was to set out basic rules and provide a generic understanding of the internet and related activities. The ITE Law set out various terms and definitions relevant for electronic transactions and introduced a number of administrative requirements to conclude digital transactions. The spirit and stated intent of the ITE Law is to protect the state, the public and the private sector against acts of cybercrimes.

The ITE Law stipulates several provisions on personal defamation, online threats and religious blasphemy. In theory, the purpose of these provisions is to enable the arrest and prosecution of cybercriminals. In reality, however, the ITE Law has been used prosecute individuals for alleged criminal actions online. Provisions of the ITE Law have frequently been used by regional and central government authorities as the legal basis to prosecute citizens who have used the internet to criticise or protest about government policies.

As the information technology sector continued to evolve, the Indonesian government sought to keep pace by issuing implementing regulations for the ITE Law and, in 2016, it amended the ITE Law itself. With the issuance of Law No. 19 of 2016, the Indonesian government amended several articles in the ITE Law and added a number of new provisions. One of the most controversial amendments was a provision that authorised the government, through the Ministry of Communication and Information (MOCI), to block websites. Despite the objections of some experts, who argued that blocking websites should only be done by way of a court order in order to limit the possibility of any abuse of power, the government is now fully authorised to block websites without any preliminary assessment.

This controversy aside, some parties applauded the ITE Law amendment for providing clearer guidelines on the appropriate use of social media. The Indonesian government seems to have decided to take a more liberal approach to regulating internet activities, with the expectation that users are able to self-regulate their internet use.

Legislation

2 What legislation governs business on the internet?

- Law No. 11 of 2008 as amended by Law No. 19 of 2016 on Electronic Information and Transactions or the ITE Law;
- Law No. 8 of 1999 on Consumer Protection (Consumer Protection Law)
- Government Regulation No. 82 of 2012 on the Implementation of Electronic Systems and Transactions (Electronic Transaction Regulation);
- MOCI Regulation No. 36 of 2014 on Procedures for the Registration of Electronic System Providers (MOCI NO. 36/2014);
- MOCI Regulation No. 20 of 2016 on the Protection of Private Data in Electronic Systems (Data Privacy Regulation);
- MOCI Regulation No. 23 of 2013 on the Management of Domain Names (Domain Name Regulation);
- MOCI Regulation No. 19 of 2014 on the Handling of Websites that Contain Negative Content (MOCI No. 19/2014);
- MOCI Regulation No. 7 of 2016 on the Administration of the Investigation and Prosecution of Criminal Acts in the Field of Information Technology and Electronic Transactions (MOCI No. 7/2016);
- Ministry of Trade (MOT) Regulation No. 86/M-DAG/PER/12/2016 of 2016 on Requirements for Licensing Services in the Field of E-Commerce Trading and Digital Signatures (MOT No. 86/2016);
- Ministry of Transportation (MOTR) Regulation No. 108 of 2017 on the Organization of Non-Fixed Route Public Transportation Services (Transportation Regulation);
- Bank Indonesia (BI) Regulation No. 20/6/PBI/2018 on Electronic Money (E-Money Regulation);
- BI Regulation No. 18/40/PBI/2016 regarding Payment Transaction Processing Operations (BI Reg 18/2016);
- Financial Services Authority (Otoritas Jasa Keuangan (OJK)) Regulation No. 77/POJK.01/2016 on Information Technology-Based Money Lending Services (Money Lending Regulation)
- Presidential Regulation No. 74 of 2017 on E-Commerce Roadmap (E-Commerce Roadmap);
- Presidential Regulation No. 44 of 2016 on List of Closed Business Activities and Business Activities Open with Requirements in the Field of Capital Investment (Negative Investment List);
- Chairman of the Capital Investment Coordinating Board (Badan Koordinasi Penanaman Modal (BKPM)) Regulation No. 13 of 2017 on Guidelines and Procedures for Capital Investment Licensing and Facilities (BKPM Regulation); and
- MOCI Circular Letter No. 5 of 2016 on Limitations and Liabilities of Platform Providers and Merchants in Conducting Electronic Commerce in the Form of User-Generated Content (Circular Letter 5/2016).

Regulatory bodies

3 Which regulatory bodies are responsible for the regulation of e-commerce, data protection and internet access tariffs and charges?

- BI;
- MOCI;
- Ministry of Industry (MOI);
- MOT;
- Ministry of Transportation (MOTR); and
- other technical government bodies and institutions relevant to the type of internet-based business.

Jurisdiction

4 What tests or rules are applied by the courts to determine the jurisdiction for internet-related transactions or disputes in cases where the defendant is resident or provides goods or services from outside the jurisdiction?

Principally, the ITE Law is applicable to any individual who carries out a certain legal action (as specified in the ITE Law) either in or outside Indonesian jurisdiction.

In the event of a dispute, the Indonesian courts shall refer to the ITE Law to determine the competent jurisdiction. For this purpose, the relevant Indonesian court shall use the definition of 'individual' stipulated in the ITE Law, namely, a natural person holding Indonesian or foreign citizenship, which also includes local and/or foreign legal entities.

Considering that the utilisation of information technology is cross-territorial in nature, it is likely that a foreign citizen or foreign legal entity would be subject to the provisions of the ITE Law to the extent that the concerned legal action had certain legal consequences in Indonesia.

Contracting on the internet

5 Is it possible to form and conclude contracts electronically? If so, how are contracts formed on the internet? Explain whether 'click wrap' contracts are enforceable, and if so, what requirements need to be met.

It is possible in Indonesia for parties to agree and enter into a digital agreement. In principle, a digital agreement shall be deemed valid if:

- there is mutual consent of the parties;
- it is concluded by a competent subject of the law or represented according to the prevailing laws and regulations;
- it is executed for a certain matter; and
- the object of the transaction is not prohibited by law, morality or public order.

A digital agreement should at least contain information on:

- the identity of the parties;
- the object of the agreement and its specifications;
- the electronic transaction requirements;
- the price and fees;
- the procedure to terminate the agreement; (vi) a provision that grants a right to the damaged party to receive indemnification for any hidden defect; and
- the choice of law to settle the electronic transaction.

Current Indonesian laws and regulations do not specifically address whether 'click wrap' contracts are enforceable in Indonesia. Since 'click wrap' contracts are prepared in digital format, such contracts should at least contain the information above to be enforceable.

Parties to a digital agreement can use a digital signature. The Indonesian government acknowledges that a digital signature is equally valid as a physical signature. A digital signature shall also be treated as having equal legal force as a physical signature.

6 Are there any particular laws that govern contracting on the internet? Do these distinguish between business-to-consumer and business-to-business contracts?

The practice of entering into digital contracts is generally regulated under the Electronic Transaction Regulation. A digital contract can be entered into by a natural person and business entity, either in the form of a legal entity or a non-legal entity. In the private sector, electronic transactions can be concluded among and between

- businesses;
- businesses and consumers;
- individuals;
- institutions; and
- institutions and businesses in accordance with the applicable laws and regulations.

Nothing in the Electronic Transaction Regulation provides any specific distinction or special treatment if the digital contract is entered into by and between business entities.

7 How does the law recognise or define digital or e-signatures?

Indonesia acknowledges digital signatures or e-signatures as a valid signature, regulated by the Electronic Transaction Regulation. Under the Electronic Transaction Regulation, a 'digital signature' is defined as a signature with electronic information attached, associated or related to other electronic information used as a tool for verification and validation purposes.

A digital signature shall have a legal binding force to the extent that:

- the data used in forming the digital signature only relates to the signatory;
- the data used in forming the digital signature during the signing process should only be under the control of the signatory;
- there is a certain method to identify the signatory; and
- there is a method to indicate that the signatory has given his or her consent to the related electronic information.

There are two types of digital signature recognised in Indonesia. These are certified digital signatures and uncertified digital signatures. A certified digital signature is created by procuring the services of an electronic certification provider and is confirmed by an electronic certificate. An uncertified digital signature is created without engaging the services of an electronic certification provider.

8 Are there any data retention or software legacy requirements in relation to the formation of electronic contracts?

The implementation of an electronic transaction in Indonesia shall comply with several requirements, one of which is to retain the relevant data domestically. The data of a signatory should be stored in a domestic facility that uses a trustworthy system owned by the digital signature provider and which is able to detect changes to the information. A trustworthy system shall be regarded as a system that follows procedures for the use of a digital signature that confirms it is genuine and the integrity of the electronic information.

In addition to the obligation to retain the data domestically as described above, electronic system providers shall guarantee that their software does not contain any unusual or hidden instructions that can be construed as a violation of the law. For example, instructions to detonate a time bomb, virus, Trojan horse, worm or backdoor. Electronic system providers that retain source code escrow, in cooperation with trusted third parties, shall take reasonable efforts to mitigate these occurrences by checking the source code.

Security

9 What measures must be taken by companies or ISPs to guarantee the security of internet transactions? Is encryption mandatory?

By regulation, an electronic system provider is obligated to guarantee the security of the software used to facilitate and administer the electronic system services, as well as to assure that an information security agreement is available. In practice, an electronic system provider is required to establish a security system that has a system and procedure for countermeasures and prevention of threats and attacks that could lead to disruptions, failure and financial loss for users.

10 As regards encrypted communications, can any authorities require private keys to be made available? Are certification authorities permitted? Are they regulated and are there any laws as to their liability?

The government is obligated to prevent the distribution and use of electronic information or documents that contain prohibited materials pursuant to the prevailing laws and regulations. To prevent such distribution and use, the government is authorised to cut access or have electronic system providers cut off access to any electronic information or document that contains prohibited materials.

The ITE Law also recognises that government officials have certain authorities to investigate criminal acts or potential criminal acts in the field of electronic transactions and information. Such authorities include:

- to receive reports on criminal acts in the field of electronic transactions and information;
- to summon the relevant parties for further investigation;

- to investigate the facts related to reports of alleged criminal acts;
- to investigate the party that is claimed to have committed the alleged criminal act;
- to examine the tools used in performing the alleged criminal act;
- to search certain locations where the alleged criminal act was committed;
- to confiscate the tools used to perform the alleged criminal act;
- to make electronic information or data related to the criminal act inaccessible;
- to request information in the electronic system or information produced by the electronic system that is relevant to the criminal act; and
- to request experts as necessary to investigate the criminal act.

Domain names

11 What procedures are in place to regulate the licensing of domain names? Is it possible to register a country-specific domain name without being a resident in the country?

Registration of a domain name is administered on a first-come, first-served basis. The process, which is quite straightforward, is initiated by the domain name user submitting an application along with the required supporting documents to the domain name registrar. The domain name registration process should not take more than five business days after a completed domain name registration is submitted and received by the domain name registrar. A non-resident can file a domain name registration application after going through the evaluation process to confirm that the foreign application complies with the administrative and financial requirements to be eligable for an Indonesian domain name.

12 Do domain names confer any additional rights beyond the rights that naturally vest in the domain name?

There are no additional rights vested in domain name users, except for the right of domain name users to transfer the domain name registration to another domain name user.

13 Will ownership of a trademark assist in challenging a 'pirate' registration of a similar domain name?

According to the Domain Name Regulation, an international holder of a trademark that has been registered in Indonesia is entitled to register, use, and benefit from the Indonesian domain name. The registration of a domain name by an international trademarked organisation should be done through an Indonesian entity by way of power of attorney.

The Domain Name Regulation does not require submission of a trademark licence to register a domain name. Although that is the case, in practice, valid evidence of trademark ownership is helpful as a supporting document when a registrar receives two applications for registration that contain similar domain names. Submitting evidence of trademark ownership is also helpful in deciding which of the two applications will be deemed a 'pirate' registration.

Advertising

14 What rules govern advertising on the internet?

There is no specific rule that governs online advertising activities. Considering that online advertising is part of an electronic transaction, such advertising is subject to the provisions of the ITE Law, the Electronic Transaction Regulation and other relevant regulations on internet-based activities.

In relation to capital investment restrictions, the Negative Investment List stipulates that activities concluded using an electronic system, including online-based advertisements, are subject to a maximum 49 per cent foreign ownership if the investment value is less than 100 billion Indonesian rupiah.

The Electronic Transaction Regulation only provides that an electronic system provider shall formulate a feature for the purpose of accessing information regarding advertisements.

15 How is online advertising defined? Could online editorial content be caught by the rules governing advertising?

There is no specific definition of 'online advertising' provided in the applicable laws and regulations in Indonesia, because online advertising is deemed an inseparable part of an electronic transaction. Online advertising activity is useful for merchants to introduce and promote their products and services. However, there are also companies established with the sole purpose of conducting online advertising services. These companies profit by designing advertisement materials, distributing those materials to numerous platforms and arranging for the ads to be published. It is unlikely for online editorial content to be classified as online advertising, since online editorial content may not necessarily be intended for commercial purposes.

16 Are there rules against misleading online advertising?

The Consumer Protection Law provides that any business entity that uses misleading information for online advertisement purposes could face imprisonment for a maximum period of five years or fined up to a maximum of 1 billion Indonesian rupiah.

17 Are there any products or services that may not be advertised on the internet?

According to the applicable laws and regulations, products or services that are not allowed to be advertised or distributed through the internet include obscene content, gambling-related content, defamatory material and blackmail-related content.

18 What is the liability of content providers and parties that merely host the content, such as ISPs? Can any other parties be liable?

If the content providers merely host the content, then their liability would be limited to the information indicated within the relevant content. If the content is unlawful, but remains unpublished, then the content providers will be solely liable. However, if unlawful content is published on a website, the relevant internet system provider can also be held liable if it cannot prove that its system is not classified as a user-generated electronic system. If it is published in a non-user generated electronic system, the internet system provider would have to decide whether the content is lawful before publishing.

Financial services

19 Is the advertising or selling of financial services products to consumers or to businesses via the internet regulated, and, if so, by whom and how?

No specific regulation on the advertisement or selling of financial services products has been issued by the Indonesian government. Hence, this topic is covered under the ITE Law and its implementing regulations.

Defamation

20 Are ISPs liable for content displayed on their sites?

As a general rule, an electronic system provider must maintain a reliable and secure electronic system. Under the ITE Law, an electonic system provider shall be held responsible for the operation of its electronic system. However, in practice, it is difficult for system providers to entirely supervise the content displayed on websites, especially if it involves a user-generated electronic system. In order to address this issue, the MOCI issued Circular Letter 5/2016, which basically provides that although providers are to be held responsible for the organisation of their platforms, said providers will no longer be held liable if they can prove that the disadvantageous action in question on their platforms was caused by users.

21 Can an ISP shut down a web page containing defamatory material without court authorisation?

The system provider is under the obligation to have a mechanism to delete electronic information that becomes irrelevant in accordance with the prevailing laws and regulations. Initially, the ITE Law provided that a system provider could only delete certain content based on a court order. The government seems to have removed the requirement to obtain a court order through the issuance of Circular Letter 5/2016. The system provider is now required to delete or block any defamatory material after it receives a report on the existence of such material.

Update and trends

The Indonesian government is in the process of revising the Electronic Transaction Regulation. The MOCI has said that such revision to the Electronic Transaction Regulation is now complete and will soon be introduced to the public for discussion. According to recent news reports, one of the main revisions concerns data, which may be categorised as either strategic or non-strategic data. Strategic data would be considered as high-risk data that must be processed, maintained and stored within the territory of Indonesia as a breach of which could harm the country. In general, the revision to the Electronic Transaction Regulation will focus on the data of users instead of the current focus on the location of the data centre.

Further, governmental institutions, law enforcers and the general public may submit a report to the MOCI so that specific websites may be blocked due to unlawful content. On receiving a report, the MOCI will add the reported website to the TRUST+ Positive list, which is a database of websites with negative content. Internet service providers must block access to all websites on the TRUST+ Positive list. This blocking can be performed independently by the internet service provider itself or through a blocking service provider. Internet service providers that fail to block websites on the TRUST+ Positive list may be subject to criminal and administrative sanctions

Intellectual property

22 Can a website owner link to third-party websites without permission?

Based on Indoneian laws and regulations, a website shall be regarded as an intellectual property of the system provider that has gathered the electronic information and documents to establish the website. In theory, a website owner has no intellectual property rights over the content displayed by another provider. If one intends to insert a link to access a third-party's website, then permission from the operator of the website is advisable even if the content of such third-party's website does not contain materials that may violate the applicable laws and regulations.

23 Can a website owner use third-party content on its website without permission from the third-party content provider? Could the potential consequences be civil in nature as well as criminal or regulatory?

In practice, many website owners use content owned by other website owners without any permission. As long as the relevant content is used for lawful purposes, the potential consequence would only be civil in nature. However, if the content has indications of, for example, gambling activities, then it could be subject to criminal sanctions.

24 Can a website owner exploit the software used for a website by licensing the software to third parties?

There is no restriction on a website owner or a electronic system provider cooperating with third parties for the purpose of exploiting software. However, it is important to note that the website owner should first confirm whether the relevant third parties are trustworthy, because a website owner is under the obligation to protect the confidentiality of source code attached to the software.

25 Are any liabilities incurred by links to third-party websites?

If links to third-party websites are displayed, then the relevant owner of the website would automatically be liable for the content of such third-party website. The owner of the website will not be liable if there is an agreement among the website owners that contains a provision that the original website owner shall be liable for any transmission of the content used on its website.

26 Is video content online regulated in the same way as TV content or is there a separate regime?

Video content accessible through a website is regulated under the same regime as other forms of electronic information or document, since the definition of electronic information or document in the ITE Law is very broad. As such, there is no special treatment or exemption for video content that is available online and publicly accessible.

27 Do authorities have the power to carry out dawn raids and issue freezing injunctions in connection with IP infringement?

With the issuance of MOCI Regulation No. 7/2016, the relevant authorities are only able to carry out dawn raids and conduct an arrest if the actions are considered as criminal activities under the electronic information technology regime. As to intellectual property infringement, the most aggressive sanction that can be imposed is the suspension of the provider's website for a certain period of time.

28 What civil remedies are available to IP owners? Do they include search orders and freezing injunctions?

See question 27.

Data protection and privacy

29 How does the law in your jurisdiction define 'personal data'?

The Data Privacy Regulation defines personal data as certain individual data, the authenticity of which is verified, sustained and maintained while its confidentiality remains protected.

30 Do parties involved in the processing of personal data, such as website owners, have to register with any regulator to process personal data?

Any personal data may only be used within the certified electronic system and it must at all times be protected during the implementation of the personal data management activities.

31 Could data protection laws and regulatory powers apply to organisations or individuals resident outside of the jurisdiction?

Any transfers of personal data from a domestic entity to a foreign country must be coordinated via the MOCI in accordance with the prevailing laws and regulations for cross-border exchanges of personal data.

32 Is personal data processed on the basis of customer consent or other grounds? What is the commonly adopted mechanism for obtaining customer consent or establishing the other grounds for processing?

Personal data can be managed by an entity based on written consent of the owner. By maintaining such consent, an entity is entitled to legally undertake the receipt, collection, processing, analysis, saving, display, announcement, transmission, dissemination, opening of access and deletion of such personal data.

33 May a party involved in the processing of personal data, such as a website provider, sell personal data to third parties, such as personal data about website users?

Indonesian legislation does not recognise personal data as a commodity that can be used for trading purposes. By definition, the ownership of personal data will always be attached to the relevant individual. In theory, however, if the individual has consented to his or her personal data being transferred, that particular transfer should be deemed as lawful.

34 If a website owner is intending to profile its customer base to carry out targeted advertising on its website or other websites visited by its customers, is this regulated in your jurisdiction?

There is no specific rule regarding technical activities that relate to personal data in Indonesia. However, the profiling of customers to be used for targeted advertising by a website owner would still be lawful if the website owner upholds the confidentiality principles adopted by the Data Privacy Regulation.

35 Does your jurisdiction have data breach notification or other cybersecurity laws specific to e-commerce?

The Data Privacy Regulation provides that in cases of failure to keep personal data confidential, the relevant electronic system provider

should notify the owner of the personal data within a maximum of 14 days as of the date such failure becomes known to the provider.

36 Does your jurisdiction recognise or regulate the 'right to be forgotten'?

Indonesia recognised the 'right to be forgetton' in 2016 through the issuance of an amendment to the ITE Law. Only the relevant user can submit an application to erase electronic information or documents, and the application should be addressed to the relevant competent court.

Electronic system providers must provide a mechanism to erase electronic information or documents, and they should erase the concerned electronic information or documents upon receiving a court order.

37 What regulations and guidance are there for email and other distance marketing?

Indonesia does not have any specific rules on email. The definition of 'electronic information' provided in the ITE Law includes email.

38 What rights and remedies do individuals have in relation to the processing of their personal data? Are these rights limited to citizens or do they extend to foreign individuals?

The individuals who own the personal data have the right to report the failure to process their personal data. The right to file a report is intended to allow negotiations between the parties to reach an amicable agreement. The Data Privacy Regulation does not specify whether 'owner of personal data' includes foreign citizens.

Taxation

39 Is the sale of online products subject to taxation?

Yes, the sale of online products is subject to taxation. Indonesian law does not specify any tax exemption for the sale of products through online systems.

40 What tax liabilities ensue from placing servers outside operators' home jurisdictions? Does the placing of servers within a jurisdiction by a company incorporated outside the jurisdiction expose that company to local taxes?

An operator should be treated as a resident taxpayer and subject to local tax laws in the jurisdiction where the server is placed, provided that the tax treaty signed between the relevant countries indicates that the placement of a server constitutes a permanent establishment.

41 When and where should companies register for VAT or other sales taxes? How are domestic internet sales taxed?

Companies classified as taxable entrepreneurs (ie, they have an annual sales revenue of more than 4.8 billion Indonesian rupiah) must pay and report VAT by way of e-filing at the end of each month. As mentioned in question 39, Indonesian tax laws do not provide any special treatment or exemption to the imposition of applicable taxes for transactions concluded online. Hence, transactions concluded through an online system are subject to VAT and income tax.

42 If an offshore company is used to supply goods over the internet, how will returns be treated for tax purposes? What transfer-pricing problems might arise from customers returning goods to an onshore retail outlet of an offshore company set up to supply the goods?

Assuming that the goods are imported from an offshore company to Indonesia, they will be subject to import duty. If those goods are returned to the offshore company, they will be considered as exports, subject to 0 per cent VAT and the relevant reporting requirements, which are the obligation of the importer.

If the offshore company delivers the goods directly to Indonesian customers, there should be no VAT payable to the local entity, in which case, the local entity will not pay VAT to the offshore entity for obtaining the goods. Consequently, the onshore company is not obligated to file a monthly VAT report with the tax office.

We do not foresee any transfer pricing problems, provided that the offshore and onshore companies do not have any special relationship. A special relationship is deemed to exist in the following circumstances, pursuant to article 18(4) of Law No. 36/2008 on Income Tax:

- where a taxpayer directly or indirectly holds 25 per cent or more of the capital of another taxpayer, or where a company holds 25 per cent or more of the capital of two taxpayers, in which case, the latter two taxpayers are also considered to be related parties;
- where there is control through management or the use of technology, even if an ownership relationship is not present; or
- where there is a family relationship, either through blood or through marriage within one degree of direct or indirect lineage.

Gambling

43 Is it permissible to operate an online betting or gaming business from the jurisdiction?

It is not permitted as gambling is strictly prohibited under Indonesian law.

44 Are residents permitted to use online casinos and betting websites? Is any regulatory consent or age, credit or other verification required?

Since the ITE Law applies cross-border to jurisdictions all over the world, a resident would be prohibited from participating in online casinos and betting websites.

Fahrul S Yusuf **fahrulyusuf@ssek.com**
Mohammad K Bratawijaya **mohammadbratawijaya@ssek.com**

14th floor, Mayapada Tower
Jl Jend Sudirman Kav 28
Jakarta 12920
Indonesia

Tel: +62 212 9532000
Fax: +62 215 212039
www.ssek.com

Outsourcing

45 What are the key legal and tax issues relevant in considering the provision of services on an outsourced basis?

There are only certain services or activities, considered as non-core activities, that can be outsourced to other companies. If an outsourcing arrangement is put in place for core business activities, the outsourcing agreement will be deemed null and void.

46 What are the rights of employees who previously carried out services that have been outsourced? Is there any right to consultation or compensation, do the rules apply to all employees within the jurisdiction?

The employees who have been replaced by way of termination due to their positions being outsourced is entitled to termination benefits.

Online publishing

47 When would a website provider be liable for mistakes in information that it provides online? Can it avoid liability?

A website provider could be held liable if a user uses false information on its website. However, the website provider can avoid such liability if it can prove that its system is a user-generated system over which it has limited control over the content published by users. In this case, it is possible that the user would be liable for mistakes in information provided online.

48 If a website provider includes databases on its site, can it stop other people from using or reproducing data from those databases?

A database should be fully controlled by the website provider. One of the obligations of a website agent provider is to confirm the control over authorisation and access rights to the database and the electronic transaction.