International
Comparative
Legal Guides

Practical cross-border insights into cybersecurity

Cybersecurity 2023

Sixth Edition

Contributing Editor:
Edward R. McNicholas
Ropes & Gray LLP

ICLG.com

Expert Analysis Chapters

Q&A Chapters

Portugal


Jorge Silva Martins


Joana Avelino Gomes


Inês Coré

CS'Associados

1 Cybercrime

1.1 Would any of the following activities constitute a criminal or administrative offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)
Yes. Hacking is a criminal offence pursuant to Article 47 of Law No. 58/2019, of 8 August 2019 (the "Portuguese Data Protection Act"). Under that article, whoever, without due authorisation or justification, accesses personal data by any means shall be subject to imprisonment of up to one year or a fine of up to 120 days.

Denial-of-service attacks
Yes. A DOS attack is a criminal offence under Article 4 of Law No. 109/2009, of 15 September 2009, as amended (the "Cybercrime Act").

Pursuant to that article, whoever, without legal permission or authorisation from the owner or holder of the right over the full system, or part thereof, deletes, alters, fully or partially deteriorates, damages, suppresses, or renders unusable or inaccessible programs or other computer data of third parties or by any other means affects their usability, shall be subject to imprisonment of up to three years or a fine.

Where high-value damage is caused, offenders shall be subject to imprisonment of up to five years or a maximum fine of 600 days.

Where considerable high-value damage is caused, offenders face imprisonment of between one and 10 years.

Attempting to commit a DOS attack is also punishable.

Phishing
Yes. Phishing is a criminal offence both under the terms of the Portuguese Criminal Code and the Portuguese Cybercrime Act.

With regard to the former, phishing constitutes IT fraud. As per Article 221 of the Portuguese Criminal Code, whoever, with the intent of obtaining unlawful enrichment, for themselves or for a third party, causes pecuniary loss, for another person by interfering in the result of data processing, incorrect structuring of computer programs, the incorrect or incomplete use of data, the unauthorised use of data or unauthorised interference by any other means in the processing, faces imprisonment of up to three years or a fine.

In the case of the latter, phishing is also punished as unauthorised access, in accordance with Article 6 of the Cybercrime Act. In this regard, the Portuguese legislator has determined that whoever, in any way, accesses a computer system without the legal permission or authorisation of the owner or holder of the right over the full system, or part thereof, faces imprisonment of up to one year or a fine of up to 120 days.

Whenever the unauthorised access is carried out to obtain data related to payment cards or any other devices that provide access to a system or payment method, the prison sentence may be increased to up to two years or a fine up to 240 days.

Attempting to commit the offence is punishable in the case of both criminal offences.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)
Yes, it is a criminal offence under the Cybercrime Act.

According to Article 5, whoever, without legal permission or authorisation from the owner or holder of the right over the full system, or part thereof, obstructs, prevents, interrupts or seriously disrupts the functioning of a computer system by introducing, transmitting, deteriorating, damaging, altering, deleting, preventing access or suppressing programs or other computer data, or by any other means interferes with a computer system, is subject to imprisonment of up to five years or a maximum fine of 600 days.

Attempting to commit this offence is also punishable.

Distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime
The distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime constitutes a form of cyber sabotage, a criminal offence under the Cybercrime Act.

Whoever unlawfully produces, sells, distributes or otherwise disseminates or introduces, into one or more computer systems, devices, programs, or other computer data intended to commit a cybercrime, is subject to imprisonment of up to five years and a fine of up to 600 days.

Possession or use of hardware, software or other tools used to commit cybercrime
Please see the answer above.

Identity theft or identity fraud (e.g. in connection with access devices)
In Portugal, identity theft is not itself classified as a crime. As a matter of fact, only the consequences of such conduct (e.g. computer forgery, defamation, invasion of privacy) would constitute a crime.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)
Article 195 of the Portuguese Criminal Code establishes that whoever, without consent, discloses another party's secrets of which they became aware due to their situation, occupation, job, profession or art, will face imprisonment of up to one year or a fine of up to 240 days.

Unsolicited penetration testing (i.e. the exploitation of an IT system without the permission of its owner to determine its vulnerabilities and weak points)
The crime of illegal/unlawful access essentially covers what has been referred to as "computer hacking".

Anyone who, without legal grounds for doing so, in any way accesses a computer system is subject to imprisonment of up to one year or with a fine of up to 120 days.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data
It is also worth highlighting Article 7 of the Cybercrime Act.

According to this provision, whoever, without legal permission or authorisation from the owner or holder of the right over the full system, or part thereof, intercepts by technical means transmissions of computer data to, from or within a computer system, shall be subject to imprisonment of up to three years or a fine.

Attempting to commit this offence is also punishable.

1.2 Do any of the above-mentioned offences have extraterritorial application?

According to Article 27 of the Portuguese Cybercrime Act, anyone who commits a crime in Portuguese territory will be subject to the provisions of Portuguese law. If, depending on the applicability of Portuguese criminal law, the Portuguese courts and the courts of another Member State of the European Union have concurrent jurisdiction to hear one of the crimes provided for in this law and, in either of them, criminal proceedings may be validly commenced or continued on the basis of the same facts, the competent judicial authority shall have recourse to the bodies and mechanisms established within the European Union to facilitate cooperation between the judicial authorities of the Member States and the coordination of their respective actions, with a view to deciding which of the two States will initiate or continue the proceedings against the perpetrators of the offence, with the aim of centralising those proceedings in only one of them.

1.3 Are there any factors that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences (e.g. where the offence involves "ethical hacking", with no intent to cause damage or make a financial gain)?

The legislator did not establish any special factors that might mitigate or excuse any of the above criminal offences.

Therefore, the general principles of the Portuguese Criminal Code shall apply, considering the specificities of each case.

2 Cybersecurity Laws

2.1 *Applicable Laws*: Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, data protection and e-privacy laws, intellectual property laws, confidentiality laws, information security laws, and import/export controls, among others.

Cybersecurity legislation covers several areas of Portuguese law. The most significant applicable legislation on the subject is as follows:

1. The Portuguese Criminal Code (Decree Law No. 48/95 of 15 March 1995, as amended) with regard to criminal and administrative offences.
2. The Cybercrime Act regarding cybercrimes.
3. The Portuguese Legal Regime for Cyberspace Security (Law No. 46/2018 of 13 August 2018, transposing Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016, concerning measures for a high common level of security of network and information systems across the European Union).
4. Decree Law No. 65/2021 of 30 July 2021, which established the Legal Regime for Cyberspace Security and defines cybersecurity certification obligations under Regulation (EU) 2019/881 of the European Parliament and the Council of 17 April 2019.
5. Portuguese Law on Electronic Communications (Law No. 16/2022 of 16 August 2022, transposing Directives 98/84/EC, 2002/77/EC and (EU) 2018/1972).
6. Law No. 46/2012 of 29 August 2012, transposing the part of Directive 2009/136/EC amending Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2012, concerning the processing of personal data and the protection of privacy in the electronic communications sector, and introducing the first amendment to Law No. 41/2004, of 18 August 2004, and the second amendment to Law No 7/2004, of 7 January 2004.
7. Law No. 59/2019 of 8 August 2019, adopting the rules on the processing of personal data for the purpose of preventing, detecting, investigating or prosecuting criminal offences or the execution of criminal sanctions, transposing Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016.
8. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation or "GDPR").
9. The Portuguese Data Protection Act (which ensures the execution of the GDPR in Portugal).
10. The Portuguese Copyright and Related Rights Code (Decree Law No. 63/85 of 14 March 1985, as amended) regarding the violation of copyrights and related rights.
11. The Portuguese Industrial Property Code (Decree Law No. 110/2018 of 10 December 2018) regarding the violation of industrial property rights and trade secrets.

2.2 *Critical or essential infrastructure and services*: Are there any cybersecurity requirements under Applicable Laws (in addition to those outlined above) applicable specifically to critical infrastructure, operators of essential services, or similar, in your jurisdiction?

The Portuguese Legal Regime of Cyberspace Security foresees that the Portuguese Public Administration, the operators of critical infrastructures, operators of essential services, and digital service providers are required to comply with appropriate and proportionate technical and organisational measures to manage the risks posed to the security of the networks and information systems they use. Those measures must ensure a level of security appropriate to the risk in question, taking into account the latest technical developments. With regard to digital service providers, those measures must take into consideration: (i) the security of the systems and installations; (ii) incident handling; (iii) business continuity management; (iv) monitoring, auditing and testing; and (v) compliance with international standards.

Moreover, Decree Law No. 65/2021 provides for the following requirements to be met by the above entities:

(a) indication of at least one permanent point of contact to ensure the flow of information at an operational and technical level with the National Cybersecurity Centre (the "CNCS");
(b) designation of a security officer to manage all measures taken regarding security requirements and incident reporting;
(c) preparation of an inventory of all the essential assets for the provision of the respective services;
(d) preparation of a security plan, duly documented and signed by the security officer, containing: (i) a security policy, including a description of organisational measures and human resources training; (ii) a description of all measures taken regarding security requirements and incident reporting; (iii) the identification of the security officer; and (iv) the identification of the permanent point of contact.
(e) preparation of an annual report containing: (i) a summary description of the main activities performed regarding network and information services security; (ii) the quarterly statistics of all incidents, indicating the number and type of incidents; (iii) the aggregate analysis of security incidents with relevant or substantial impact; (iv) the recommendations of activities, measures or practices that promote the improvement of network and information systems security; (v) the problems identified and measures implemented as a result of the incidents; and (vi) any other relevant information; and
(f) performance of a risk analysis of all assets that ensure the continued operation of the networks and information systems used.

2.3 *Security measures*: Are organisations required under Applicable Laws to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

As for the processing of personal data, Law No. 59/2019 and the GDPR provide for rules on the security of processing where both controllers and processors are required to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk of the processing activities. As per the GDPR, measures shall include, as appropriate:

(a) the pseudonymisation and encryption of personal data;
(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2.4 *Reporting to authorities*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

Pursuant to the Portuguese Legal Regime for Cyberspace Security, the Portuguese Public Administration, operators of critical infrastructures, operators of essential services, and digital service providers are required to notify the CNCS of incidents with a relevant impact on the security of network and information systems, on the continuity of the essential services provided and on the delivery of digital services, respectively. In that regard, the notifications sent by the operators of critical infrastructures shall include information enabling the CNCS to determine the cross-border impact of incidents. The CNCS takes into consideration: (i) the number of users affected; (ii) the duration of the incident; and (iii) the geographical distribution with regard to the area affected by the incident to determine the scale of the incident's impact. With regard to digital service providers, the CNCS further takes into account: (iv) the severity of the disruption to the operation of the service; and (v) the extent of the impact on economic and societal activities.

According to the Portuguese Law on Electronic Communications, companies offering public electronic communications networks or publicly available electronic communications services must: (i) notify the *Autoridade Nacional de Comunicações* ("ANACOM") and the CNCS without undue delay, of any security incident with a significant impact on the operation of the networks or services; and (ii) inform the public, by the most appropriate means, of security incidents, when this is deemed by ANACOM to be in the public interest.

In accordance with Law No. 46/2012, companies providing publicly available electronic communications services are required to notify, without undue delay, the Portuguese Data Protection Supervisory Authority (the "CNPD") in the event of a personal data breach. The notification must include: (i) the identification of the nature of the personal data breach; (ii) the points of contact where further information can be obtained; (iii) a recommendation of measures to mitigate the possible adverse effects of the data breach; (iv) the consequences of the personal data breach; and (v) the measures taken to address the data breach.

As for the processing of personal data, Law No. 59/2019 and the GDPR provide for an obligation on the controller to report a personal data breach to the CNPD without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. The

notification shall, at least: (i) describe the nature of the personal data breach, including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned; (ii) communicate the name and contact details of the data protection officer or other points of contact where more information can be obtained; (iii) describe the likely consequences of the personal data breach; and (iv) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

2.5 *Reporting to affected individuals or third parties*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

As pursuant to Law No. 46/2012, and in the event of risk of a breach of the security of the network, companies providing publicly available electronic communications services are required to inform the service subscribers of such risk, free of charge. Where the risk is outside the scope of the measures to be taken by the service provider, it shall also inform the service subscribers of the possible solutions for avoiding the risk and the likely costs involved. Furthermore, if a data breach could potentially adversely affect the service subscriber´s personal data, companies providing publicly available electronic communications services are required to notify them, without undue delay. In such cases, the notification must include, at least: (i) identification of the nature of the personal data breach; (ii) the points of contact where further information can be obtained; and (iii) a recommendation of measures to mitigate the possible adverse effects of the data breach.

As for the processing of personal data, Law No. 59/2019 and the GDPR provide for an obligation on the controller to report a personal data breach to the data subjects, without undue delay, when it is likely to result in a high risk to the rights and freedoms of such natural persons. The notification must describe in clear and plain language the nature of the personal data breach, and at least: (i) communicate the name and contact details of the data protection officer or other point of contact where more information can be obtained; (ii) describe the likely consequences of the personal data breach; and (iii) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

2.6 *Responsible authority(ies)*: Please provide details of the regulator(s) or authority(ies) responsible for the above-mentioned requirements.

The competent authorities for the enforcement of the above requirements are as follows:

(a) CNCS, being responsible for supervising compliance with the Portuguese Legal Regime of Cyberspace Security and Decree Law No. 65/2021.
(b) ANACOM, being responsible for supervising compliance with Portuguese Law on Electronic Communications and Law No. 46/2012.
(c) CNPD, being responsible for supervising compliance with Law No. 46/2012, Law No. 59/2019, and the GDPR.

2.7 *Penalties*: What are the penalties for not complying with the above-mentioned requirements?

Failure to comply with the requirements provided for by the Portuguese Legal Regime of Cyberspace Security may result in administrative fines. The amount due depends on the severity of the infringement, and may range from 3,000 EUR to 50,000 EUR.

Moreover, failure to comply with the requirements provided for by the Portuguese Law on Electronic Communications may result in administrative fines ranging from 2,000 EUR to 5 million EUR.

As for the requirements provided for by Law No. 46/2012, failure to comply may result in administrative fines ranging from 5,000 EUR to 5 million EUR.

With regard to the processing of personal data, failure to comply with the requirements provided for by the GDPR may result in administrative fines of up to 10 million EUR or up to 2% of the offender's total worldwide annual turnover in the preceding financial year, whichever is higher. Failure to comply with the requirements provided for by Law No. 59/2019 may result in administrative fines ranging from 1,000 EUR to 20 million EUR or from 2% up to 4% of the offender's total worldwide annual turnover in the preceding financial year, whichever is higher.

2.8 *Enforcement*: Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

A number of investigations have been conducted, such as on GDPR compliance in Portugal. For example, CNPD applied a fine of 1.25 million EUR on the Municipality of Lisbon in December 2021 for violation of several GDPR provisions, including non-compliance with the law, violation of the principles of data minimisation and data retention, and non-compliance with transparency obligations regarding the processing of personal data of activist groups and demonstrators.

3 Preventing Attacks

3.1 Are organisations permitted to use any of the following measures to protect their IT systems in your jurisdiction (including to detect and deflect Incidents on their IT systems)?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)
The use of beacons is not prohibited under Portuguese law.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)
The use of honeypots is not prohibited under Portuguese law.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)
The use of sinkholes is not prohibited under Portuguese law.

3.2 Are organisations permitted to monitor or intercept electronic communications on their networks (e.g. email and internet usage of employees) in order to prevent or mitigate the impact of cyber attacks?

Although organisations are responsible for preventing cyber-attacks, the monitoring of electronic communications and networks such as the employees' e-mail and internet usage is only permitted under specific circumstances provided for by law. The Portuguese Labour Code (Law No. 7/2009 of 12 February 2009), for instance, prohibits employers from accessing messages of a personal or non-professional nature, where employees use the employer's means of communication. Nevertheless, the employer has the power to establish rules for the use of the organisation's means of communication, provided that means adopted to control that use comply with principles of necessity, proportionality and good faith, and that the organisation is able to demonstrate that it has chosen the means of control that have the least impact on the employees' fundamental rights. If organisations must process personal data to prevent and mitigate the impact of cyber-attacks, the GDPR will also apply.

3.3 Does your jurisdiction restrict the import or export of technology (e.g. encryption software and hardware) designed to prevent or mitigate the impact of cyber attacks?

Export restrictions may apply to dual-use items insofar as the technology to prevent or mitigate the impact of cyber-attacks can be used for both civilian and military applications, since the European Union controls the export, transit, brokering and technical assistance of dual-use items through Regulation (EU) 2021/821.

4 Specific Sectors

4.1 Does market practice with respect to information security vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

The application of market standards across business sectors is common in more heavily regulated sectors such as the financial or telecoms sectors. An example of those standards is ISO/IEC 27001 on information security management.

The CNCS has also issued technical recommendations setting out the best standards and practices to ensure the increase of organisations' cybersecurity.

4.2 Excluding the requirements outlined at 2.2 in relation to the operation of essential services and critical infrastructure, are there any specific legal requirements in relation to cybersecurity applicable to organisations in specific sectors (e.g. financial services or telecommunications)?

With regard to financial services, and as provided for by the Portuguese Legal Regime for Cyberspace Security, the banking sector and the financial market infrastructures are regarded as operators of essential services. Therefore, the requirements listed in question 2.2 apply.

In relation to telecommunications, the Portuguese Law on Electronic Communications establishes that companies providing public electronic communications networks or publicly available electronic communications services must adopt proportionate technical and organisational measures to appropriately manage the risks to security of networks and services, including, if appropriate, encryption. These measures shall, at least, take into account: (i) physical and environmental security, security of supply, network access control and network integrity; (ii) security incident management procedures, security incident detection capability, reporting and notification, public disclosure and any other communication regarding security incidents; (iii) business continuity strategy and contingency plans, and disaster recovery capabilities; and (iv) monitoring and logging policies, contingency planning exercises, network and service testing, security assessments and compliance monitoring, based on the existing national, European and international standards, specifications or recommendations on the subject.

Moreover, Law No. 46/2012 requires that companies providing publicly available electronic communications services take appropriate technical and organisational measures to safeguard the security of their services, together with the provider of the public communications network, which shall at least ensure: (i) that personal data can be accessed only by authorised personnel, and only for legally authorised purposes; (ii) the protection of personal data transmitted, stored or otherwise processed, against accidental or unauthorised destruction, loss, alteration, disclosure or access; and (iii) the implementation of a security policy with respect to the processing of personal data. Furthermore, companies providing publicly available electronic communications services shall maintain data breach records indicating: (i) the facts concerning the personal data breach; (ii) the consequences of the personal data breach; (iii) the measures taken to address the data breach; and (iv) the notifications made regarding the data breaches.

5 Corporate Governance

5.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' or officers' duties in your jurisdiction?

Applicable Laws do not provide for specific obligations nor liabilities for company's directors or officers, and therefore they may not be personally responsible for breaches of Applicable Laws by the company. Nonetheless, the Portuguese Labour Code may apply and a director or officer may be subject to sanctions if the company is fined due to his or her failure to take the appropriate measures for the company to comply with Applicable Laws.

5.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO (or equivalent); (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

Only the entities identified above at question 2.2, as previously stated, are required to: (i) designate a security officer; (ii) elaborate a security plan; and (iii) perform a risk analysis of all assets that ensure the continued operation of the networks and information systems used.

With regard to the processing of personal data, and in addition to the security measures identified above at question 2.3, the GDPR also requires that the controller and the processor designate a data protection officer ("DPO") in cases where:

(a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
(b) the core activities of the controller or the processor consist of processing operations that, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
(c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data or personal data relating to criminal convictions and offences.

5.3 Are companies (whether listed or private) subject to any specific disclosure requirements (other than those mentioned in section 2) in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

No further disclosure requirements are provided for by law other than the ones already mentioned above in section 2.

6 Litigation

6.1 Please provide details of any civil or other private actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

If failure to comply with the Applicable Laws causes material and/or non-material damages, those who have suffered from such damages may have a right to civil compensation. A civil action may be brought on several different grounds.

For instance, the GDPR establishes that any person who has suffered material or non-material damage as a result of an infringement of the GDPR shall have the right to receive compensation from the controller or processor from the damage suffered.

6.2 Please cite any specific examples of published civil or other private actions that have been brought in your jurisdiction in relation to Incidents.

There have been recently several cybersecurity attacks on fairly large companies from different sectors in Portugal. As a way of example, TAP, a state-owned civil aviation company had its computer systems undermined by a group of cyber hackers and the personal data of 1.5 million of the airline's customers was accessed and published illegitimately. On the other hand, IMPRESA, one of the largest media groups in Portugal, suffered a cyber-attack, which not only compromised personal data of the media group's clients but also blocked all the domain names hosted at IMPRESA group servers. All of these cybersecurity incidents have triggered investigations from the competent regulatory authorities but have not yet reached the civil courts, insofar as it is often nearly impossible to determine the perpetrators of such incidents.

6.3 Is there any potential liability in tort (or equivalent legal theory) in relation to failure to prevent an Incident (e.g. negligence)?

The Portuguese Civil Code (Decree Law No. 47344/66 of 25 November 1966) provides for the possibility to seek compensation for damages caused by negligence. Nevertheless, the Portuguese Civil Code is subsidiary in relation to other legislation.

7 Insurance

7.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Insurance companies are allowed to take out insurance against any risk, with the exception of: (i) criminal, administrative or disciplinary responsibility (but including civil responsibility related thereto); (ii) crimes against personal liberty (such as kidnapping or abduction) (but including compensatory damages); (iii) possession and transportation of narcotics or other forbidden drugs (but including compensatory damages); and (iv) the death of children below the age of 14 (except in certain cases) or of a mentally disabled individual.

Therefore, the risk of a cybersecurity incident can be covered by an insurance agreement under Portuguese Law.

Only insurance companies duly authorised in Portugal (or benefitting from an EU passport and complying with the relevant passport requirements) are authorised to conduct insurance business in Portugal and cover any risks in this territory.

7.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

In abstract, there are no limitations on the type of coverage that insurance companies may provide, other than the ones foreseen in question 7.1.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. anti-terrorism laws) that may be relied upon to investigate an Incident.

The authorities with investigatory powers under Applicable Laws differ according to the sector under consideration.

The authority to investigate any crime in Portugal belongs to the prosecutor's office. In some cases, the investigation depends on the complaint of the victim to the competent authorities within six months from the occurrence.

If the incident concerns any failure to comply with the requirements set out in the Applicable Laws to Public Administration, operators of critical infrastructures, operators of essential services, and digital service providers, the CNCS will be the investigative authority.

With regard to the violation of requirements imposed by Applicable Laws to publicly available electronic communications services concerning the security of networks, the investigative authority will be ANACOM.

On the other hand, if the incident concerns a personal data breach, the CNPD will be the investigative authority.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

Portuguese law does not require organisations to implement backdoors nor to provide encryption keys to law enforcement authorities.

Jorge Silva Martins heads the Technology, Data and Digital Innovation practice. With more than 15 years of experience, and a strong background in highly regulated sectors, he advises domestic and international clients on matters relating to e-commerce, electronic communications, internet law, media and audiovisual laws, intellectual property, data protection and cybersecurity. Based on his extensive experience, pragmatic approach and his ability to cut through to the key issues, he also counsels clients on the definition of innovation and business strategies, in particular in projects involving new technologies such as blockchain and artificial intelligence. Jorge is also the author of several articles in the field of technology, and a regular speaker at industry and academic conferences and presentations.

CS'Associados
Avenida da Liberdade, 249, 8º
1250-153 Lisboa
Portugal

Tel: +351 211 926 835
Email: jorge.silvamartins@csassociados.pt
URL: www.csassociados.pt

Joana Avelino Gomes is an Associate in the Criminal, Administrative Offences and Compliance practice.

CS'Associados
Avenida da Liberdade, 249, 8º
1250-153 Lisboa
Portugal

Tel: +351 211 926 835
Email: joana.gomes@csassociados.pt
URL: www.csassociados.pt

Inês Coré is a Trainee in the Technology, Data and Digital Innovation practice.

CS'Associados
Avenida da Liberdade, 249, 8º
1250-153 Lisboa
Portugal

Tel: +351 211 926 835
Email: ines.core@csassociados.pt
URL: www.csassociados.pt

ICLG.com

Current titles in the ICLG series

Alternative Investment Funds
Anti-Money Laundering
Aviation Finance & Leasing
Aviation Law
Business Crime
Cartels & Leniency
Class & Group Actions
Competition Litigation
Construction & Engineering Law
Consumer Protection
Copyright
Corporate Governance
Corporate Immigration
Corporate Investigations
Corporate Tax
Cybersecurity
Data Protection
Derivatives
Designs
Digital Business
Digital Health
Drug & Medical Device Litigation
Employment & Labour Law
Enforcement of Foreign Judgments
Environment & Climate Change Law
Environmental, Social & Governance Law
Family Law
Fintech
Foreign Direct Investment Regimes
Franchise
Gambling
Insurance & Reinsurance
International Arbitration
Investor-State Arbitration
Lending & Secured Finance
Litigation & Dispute Resolution
Merger Control
Mergers & Acquisitions
Mining Law
Oil & Gas Regulation
Patents
Pharmaceutical Advertising
Private Client
Private Equity
Product Liability
Project Finance
Public Investment Funds
Public Procurement
Real Estate
Renewable Energy
Restructuring & Insolvency
Sanctions
Securitisation
Shipping Law
Technology Sourcing
Telecoms, Media & Internet
Trade Marks
Vertical Agreements and Dominant Firms

The International Comparative Legal Guides are published by: global legal group