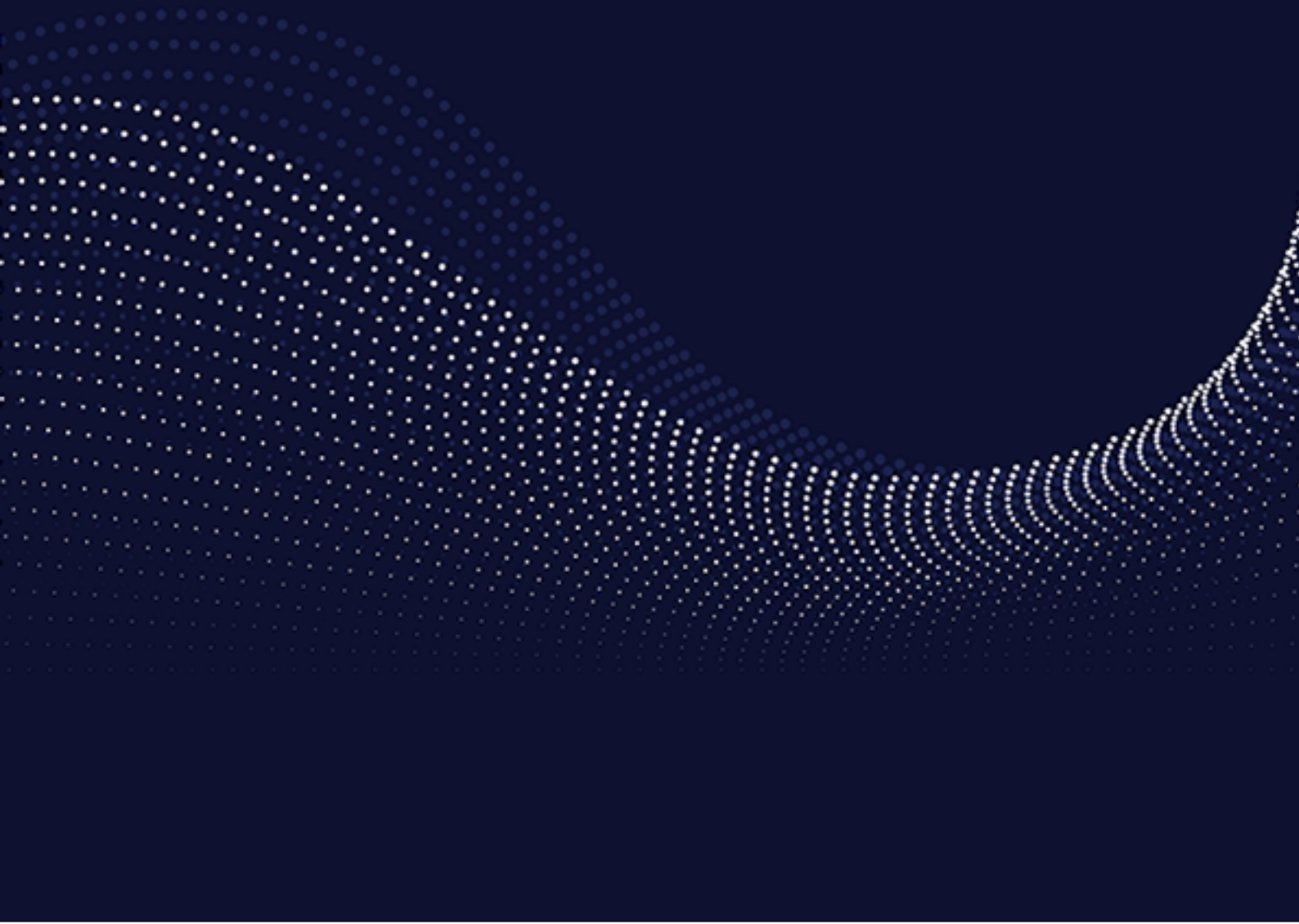
LEXOLOGY
Getting The Deal Through

DIGITAL BUSINESS 2024

Contributing Editor
Ashley Winton
Mishcon de Reya LLP



Digital Business 2024

Consulting Editor

Ashley Winton

Mishcon de Reya LLP

Quick reference guide enabling side-by-side comparison of local insights into legal and regulatory framework; contracting on the internet; security, including security of payment; domain names; advertising; financial services; defamation; intellectual property; data protection; taxation; gambling; outsourcing; online publishing; dispute resolution; and recent trends.

Generated on: October 17, 2023

LEXOLOGY
Getting The Deal Through

Portugal

Ana Rita Paínho, **Verónica Fernández**, **Teresa Pala Schwalbach**, **Rita Canas Da Silva**, **Ana Mira Cordeiro**
Sérvulo & Associados

Summary

LEGAL AND REGULATORY FRAMEWORK

Government approach

1 How would you describe the government's attitude and approach to digital content and services, digital transformation and doing business online?

The Portuguese government's attitude is globally welcoming towards these matters. Legislative initiatives in the past few years include:

- The government's INCoDe.2030 Programme – an initiative to enhance digital competences;
- Decree Law 67/2021 – a legal framework establishing Technological Free Zones (TFZs);
- Council of Ministers Resolution 29/2020 – encouraging the development of a legislative framework facilitating research, simulation and testing activities for innovative technologies, products, services and models (artificial intelligence, blockchain, virtual reality, big data, 5G, Internet of Things) by creating TFZs; and
- Council of Ministers Resolution 30/2020 – Action Plan for Digital Transition, foreseeing a strategic framework for the integration of Public Administration in the cloud.

Despite the positive attitude and evolution, still a lot more could be done in practical terms, by means of direct incentives aimed at the markets and the global public.

Legislation

2 What legislation governs digital content and services, digital transformation and the conduct of business online?

Aside from sector-specific applicable regulation, digital content and services are mostly regulated by legislation on:

- consumer protection including e-commerce/distant transactions and contracts for the supply of digital content and digital services;
- advertisement and unfair practices;
- unfair competition;
- electronic communications;
- audio-visual and media services;
- privacy;
- cybersecurity;
- authorship and related rights; and
- industrial property.

The government's 2020 Action Plan for Digital Transition and the Portuguese Charter of Human Rights in the Digital Age are also worth mentioning.

Regulatory bodies

3 Which regulatory bodies are responsible for the regulation of digital content and services, e-commerce, data protection, artificial intelligence, internet access and telecommunications?

The responsible regulatory bodies are as follows:

- Inspectorate General for Cultural Activities (IGAC): powers of supervision, control, removal and prevention of access in the digital environment to authorship and related rights, protected content over intermediary service providers.
- General Directorate of Consumer Affairs (DGC): supervisory competences in consumer protection and Laws.
- Food and Economic Safety Authority (ASAE): supervisory competences in consumer laws and overall economic activities.
- Portuguese Data Protection Authority (CNPD): supervisory powers including ePrivacy regulations.
- National Communications Authority (ANACOM): regulation of the entire communications sector, including telecommunications, with regulatory, supervisory, oversight and sanctioning powers.
- Regulatory Authority for the Media (ERC): regulation of social media platforms whenever they host or are used as broadcast media outlets.

Jurisdiction

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

In business-to-business transactions, parties are free to set choice of law and venue clauses, which will most likely be held up in Portuguese Courts. Unless otherwise agreed by the parties, the general rule under the law is that the action must be brought before the competent court in the country of residence of the defendant. For cases in which the dispute refers to provision of services to be provided in Portugal, Portuguese courts have jurisdiction.

In business-to-consumer transactions, if the plaintiff is a consumer resident in Portugal, they can choose to initiate proceedings either in Portugal, or in the EU member state in which the provider is headquartered, regardless of choice of law and venue that may be set on the underlying contract. If the contract contains a jurisdiction clause, the competent court shall be determined in compliance with the general terms of the Brussels I Regulation and

the Rome I Regulation as per the applicable law, even if one of the parties is not resident in a member state. In this case, the ultimate target is to protect the interests of the consumer and choice of law or venue (or both) is made for his or her benefit.

To date, as far as we are aware, there is no record of legal disputes on transactions in the metaverse.

Establishing a business

5 What regulatory and procedural requirements govern the establishment of digital businesses and sale of digital content and services in your jurisdiction? To what extent do these requirements and procedures differ from those governing the establishment of brick-and-mortar businesses?

No immediate differences apply to the establishment of businesses based on their digital or non-digital nature. The main exception is the online betting and gambling industry in Portugal, in which licencing schemes for operators' online or offline betting and gambling products are substantially different, as well as regulated and supervised independently.

CONTRACTING ON THE INTERNET

Contract formation

6 Is it possible to form and conclude legal contracts digitally? If so, how are digital contracts formed and are there any exceptions for certain types of contract?

As a rule, a contract whose validity is not subject to special requirements can be entered into online.

However, where the agreement itself or sector-specific laws require a handwritten signature, such agreement must be signed by means of a qualified electronic signature, as required under EU Regulation 910/2014 (the eIDAS EU Regulation). Examples include consumer financing, licence and transfers of authorship rights and protected content, contracts relating to security deposits and real estate transactions.

Applicable laws

7 Are there any particular laws that limit the choice of governing law, language of the contract or forum for disputes when entering into digital contracts? Do these distinguish between business-to-consumer and business-to-business contracts?

Yes. For business-to-consumer online contracts, pre-contractual information, including the agreement itself (T&Cs), must be presented in Portuguese and, by statutory provisions of consumer laws, regardless of what the agreement might state, the applicable law and dispute forum shall be Portuguese. Businesses also are required to offer consumers information on alternative dispute resolution (ADR) forums.

In business-to-business contracts, despite the generally accepted principle of freedom of choice and forum, a preventive case-by-case analysis based on the applicable sector specifications is recommended.

Electronic signatures

8 How does the law recognise or define digital or e-signatures? Must digital or e-signature providers be registered or licensed in your jurisdiction? What type of digital information can be signed and how does the signing take place?

Portuguese legislation follows the eIDAS EU Regulation, complemented by Decree-Law 12/2021 regarding competences and responsibilities of the State Electronic Certification System's (SECS) managing board.

Under the eIDAS EU Regulation, the provision of electronic signature services with (1) simple or standard, (2) advanced and (3) qualified different legal effects, requires pre-assessment and approval of their conformity to be included in the European Commission's Qualified Trust Service Providers list and the qualified trust services provided listed in the Portuguese Trusted List.

Breach

9 Are any special forums for dispute resolution or remedies available for the breach of digital contracts?

No. The same judicial and alternative dispute resolution methods are available for all types of contracts, regardless of their material support. Jurisdiction and competence are determined based on the subject matter and material applicable law.

FINANCIAL SERVICES

Regulation

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

Advertising and selling of such products by digital means or via the internet are not regulated in Portugal by specific legislation, but by laws and regulations applicable to the general advertising of such types of services and products. In addition to the Advertisement Code (Decree-Law 330/90), specific regulations issued by the Bank of Portugal, the Portuguese Securities Markets Commission (CMVM) and the Insurance and Pension Funds Supervisory Authority (ASF) must be observed, depending on the nature of the services or products; once such matters are subject to the regulation and supervision of said institutions.

Regarding the advertising of financial products and services subject to the supervision of the Bank of Portugal, Notice 10/2008 and Notice 5/2017 apply. All advertising materials related to public offers are subject to prior approval by the CMVM. As for insurance, Regulation 3/2010-R of ASF establishes the principles and rules to be complied with by insurance companies, intermediaries and pension fund management entities.

The sale of financial products and services, digitally or via the internet, shall also comply with the provisions of Decree-Law 95/2006 of 29 May, which transposed Directive 2002/65/EC on the distance marketing of consumer financial services.

Electronic money and digital assets

11 Are there any rules, restrictions or other relevant considerations regarding the issue of electronic money, digital assets or use of digital currencies?

Yes. According to Decree Law 91/2018 of 12 November – legal framework on payment services and electronic money (transposing Directive 2015/2366 (the PSDII)) – the issue of electronic money is restricted to the following entities:

- credit institutions having their head office in Portugal including the issue of electronic money in their corporate purpose;
- electronic money institutions having their head office in Portugal;
- credit institutions having their head office outside Portugal that are legally authorised to pursue the activity in Portugal;
- electronic money institutions having their head office in another EU member state that are authorised to operate in Portugal;
- branches of electronic money institutions having their head office outside the EU;
- the Portuguese state, autonomous regions and services and bodies under direct and indirect state government when not acting in their capacity as public authorities; and
- The European Central Bank, the Bank of Portugal and all other national central banks when not acting in their capacity as monetary authority or in the exercise of other public powers.

The law sets out the applicable procedures to be complied with by issuers of electronic money in connection with the issuance, distribution and reimbursement of electronic money. These matters are subject to a limited but significant set of conduct rules that should be taken into due account in the contractual relationship between issuers and holders of electronic money.

The issue of digital assets or use of digital currencies is not yet regulated under Portuguese legislation.

Digital and crypto wallets

I

12 Are there any rules, restrictions or other relevant considerations regarding the provision or use of crypto wallets or other methods of digitally storing value?

Yes. Further to the publication of Law 58/2020, of 31 August – which transposed the Fifth Money Laundering Directive – entities providing services allowing the safekeeping or administration of crypto actives were included within the scope of the (non-financial) entities obliged to comply with the prevention of money laundering and terrorist financing (ML/CFT) obligations under the applicable legislation, specifically Law 83/2017 of 18 August 2017, which lays down preventive and punitive measures relating to AML/CFT.

The provision of such types of services became thus subject to the prior registration of the service providers with the Bank of Portugal (under Bank of Portugal Notice 3/2021).

The Bank of Portugal has been entrusted with the responsibility for verifying compliance with the legal and regulatory provisions governing the prevention of AML/CFT by crypto wallets service providers. It should be noted that the Bank of Portugal's supervision over crypto wallet service providers is limited in scope to AML/CFT purposes, and does not cover other areas of a prudential, market conduct or any other nature.

Electronic payment systems

13 How are electronic payment systems regulated in your jurisdiction? Is there a specific law regulating third-party access to digital information in bank accounts?

Electronic payment systems are mainly regulated by Decree-Law 91/2018, which transposed PSD II. The provision of certain services that allow third-party access to digital information in bank accounts, such as Payment initiation Services (PIS) and Account information Services (AIS), is also subject to regulation by the law.

Online identity

14 Are there any rules, restrictions or other relevant considerations regarding the use of third parties to satisfy know-your-customer (KYC) or other anti-money laundering (AML) identification requirements?

Yes. Article 41 of Law 83/2017 of 18 August expressly entitles obliged entities to comply with AML/CTF obligations to use third parties to execute the identification and due diligence procedures, provided that such obliged entities:

- ensure that such third parties are qualified to perform identification and due diligence procedures as their third-party entities;
- assess, based on information in the public domain, the reputation and suitability of such third parties;
- complete the information collected by third parties or carry out a new identification, in case of insufficient information or when the associated risk justifies it;
- fulfil all document conservation requirements; and

- ensure that such third parties: (1) gather all the information and comply with all identification, due diligence and document conservation procedures with which the obliged entities themselves must comply; and (2) when requested, immediately provide a copy of the identification and identity verification data and other relevant documentation about the customer, their representatives or beneficial owners who have been subject to the identification and due diligence procedures.

DOMAIN NAMES AND URLS

Registration procedures

15 What procedures are in place to regulate the registration of domain names or use of URLs? Is it possible to register a country-specific domain name without being a resident or business in the country? Are there any restrictions around the use of URLs to direct users to particular websites, online resources or metaverses?

Registration and management of '.pt' domains is ensured by DNS.pt Association (delegated competences by the Internet Corporation for Assigned Names and Numbers (ICANN)).

Applicants' place of residence is not a requirement for registration of country-specific domain names.

With regard to embedded linking, no local specific regulations apply. However, there is an increased tendency for website and digital product owners to adopt legal disclaimers excluding liability for access to third parties' websites in view of the latest decisions by the Court of Justice of the European Union on whether directing users to third parties' websites containing IP-protected content should be regarded as a communication to the public and thus require the rights holder's prior authorisation.

IP ownership

16 Can domain names or URLs be the subject of trademark or copyright protection in your jurisdiction? Will ownership of a trademark or copyright assist in challenging a competitive use or registration of a similar domain name or URL?

No. Registration of domain names grants protection of the name as a digital asset but does not guarantee any special protection as intellectual property. However, if a domain name is the same as or similar to the reproduction of a word trademark, there may be grounds for an IP legal dispute.

Compared to the standard regime in force in the European Union, no local specificities apply.

In the event of a dispute, the most appropriate and effective mechanism is arbitration through the Arbitration Centre for Industrial Property, Domain Names, Trade Names and Corporate Names (ARBITRARE).

ADVERTISING

Regulation

17 | What rules govern online advertising?

Online advertising is subject to the same rules as offline advertising, provided for in the Advertisement Code and in Decree-Law no 57/2008 (transposing Directive 2005/29/CE, concerning unfair business-to-consumer commercial practices).

When advertisements are displayed via the use of cookies or other tracking technologies, Law 41/2004 (transposing Directive 2002/58/CE – ePrivacy Directive) shall also apply; and, if the use of cookies implies processing of personal data, then the General Data Protection Regulation (GDPR) also applies. The content of the advertisement is subject to the Advertising Code and, in the case of regulated industries (eg, financial services), any relevant specific provisions.

On 25 January 2022, the Portuguese Data Protection Authority (CNPD) issued Guideline/2022/1 on electronic direct marketing communications, under which data subjects must be able to provide consent specifically, entity by entity, even with regard to companies within the same corporate group or affiliates, otherwise the consent cannot be deemed as valid, nor all subsequent data processing activities engaged on that data collected on the legal grounds of consent.

Under this guideline: (1) as most direct marketing activities involve large-scale data processing and frequently use innovative technologies, a DPIA may be required; and (2) controllers must maintain an up-to-date list of persons who have expressly and freely given their consent to receive marketing communications, as well as clients who have not objected to receiving it, under the ePrivacy Directive.

Members of the Portuguese Advertising Self-Regulation Association are also bound by their own code of conduct and guidance on marketing communications and online behavioural advertising.

Online advertisement on the metaverse is not yet subject to specific requirements.

Targeted advertising and online behavioural advertising

18 | What rules govern targeted advertising and online behavioural advertising? Are any particular notices or consents required?

Most targeted and online behavioural advertising practices in digital environments result from the use of cookies or other tracking technologies. Thus, Law 41/2004 (transposing Directive 2002/58/CE – ePrivacy Directive) shall apply and, where the use of cookies implies processing of personal data, the GDPR also applies.

Such practices require the user's prior consent, collected based on the GDPR criteria and requirements.

Misleading advertising

19 | Are there rules against misleading online advertising?

Online advertising follows the general rules of the Advertisement Code (Decree-Law 330/90) and Decree-Law 57/2008 (transposing Directive 2005/29/CE). There are no specific rules applicable to online advertising, or industry-specific rules, as rules are general and apply to any form of advertising, regardless of the medium used for its dissemination.

All claims regarding the origin, nature, composition, properties and acquisition of goods or services advertised must be accurate and verifiable at all times. Advertisers are advised to keep evidence of all these elements. Advertisement communications containing false information, or even truthful content that leads or may lead the consumers to errors in perception, is deemed misleading advertising. Advertisement communication omitting information in such a way that the consumer is misled is also deemed misleading and is thus forbidden.

Restrictions

20 | Are there any digital products or services that may not be advertised online?

Advertising restrictions are based on the nature of the specific products (alcohol, tobacco, medical treatments or medicines, products containing high energy value, salt content, sugar, saturated fatty acids and processed fatty acids, gambling, pornography, etc) or the advertising targets (specifically minors or made in the vicinity of schools), not by the media through which the advertising is communicated.

Direct email marketing

21 | What regulations and guidance apply to email, SMS and other direct marketing?

Distance marketing practices are regulated by Law 41/2004 (transposing Directive 2002/58/CE – ePrivacy Directive) and by the GDPR, while the content is subject to the Advertising Code, as well as, in the case of regulated industries (eg, financial services), any relevant specific provisions.

Members of the Portuguese Advertising Self-Regulation Association are also bound by the association's own code of conduct and guidance on marketing communications.

In line with the ePrivacy Directive, unsolicited marketing communications require the individual's prior, explicit and specific consent, except where it is sent by data controllers with whom they have a previous commercial relationship, and advertising similar products or services to those previously transacted. In such cases, data subjects must be granted the right to object at any time, easily and free of charge, to receiving direct marketing

communications. These rules apply to all messaging systems potentially used for direct marketing.

The Portuguese Data Protection Authority (CNPD) recently issued Guideline/2022/1 on personal data protection and privacy in communications, which stresses these principles and where practical examples of (non) admissible practices are provided.

ONLINE PUBLISHING

Hosting liability

22 What is the liability of internet service providers, telecommunications providers and other parties that merely host and display the content written or published by third parties? How can these providers minimise their liability?

Liability of content providers and mere hosts (such as ISPs) follows the general rules on the attribution of liability, in addition to the rules provided by Decree law 7/2004 on e-commerce on the internal market and processing of personal data (transposing Directive 2000/31/CE).

Under these principles, the party directly responsible for the creation of the (illegal) content is ultimately responsible for the damages it may cause. With regard to ISPs, there is a general principle of absence of duty of supervision of the content provided, not being subject to a general obligation to monitor the information they transmit or store or to investigate any illicit activities carried out within their scope.

Thus, ISPs that only carry out the activity of transmitting information on a network, or providing access to a communications network, without being at the origin of the transmission or intervening in its content, are exempt from all responsibility for the information or content transmitted.

Nonetheless, according to EU Regulation No. 2022/2065 of 19 October on the single market for digital services, such responsibility exemption only exists as long as the internet service provider:

- does not have effective knowledge of the illegal content or activity, and
- once they acquire such knowledge, diligently acts to suppress or deactivate the access to the illegal content.

On the other hand, internet service providers must ensure that mechanisms are available that allow users to easily report illegal content, so that the provider can have knowledge of, and act upon, the illegal content.

Nonetheless, Decree Law 84/2021 (transposing Directive 2019/770 (the DSM Directive)) assigns an active role in preventing copyright infringement to ISPs, who must seek to obtain prior authorisation for the use of protected content, for instance by entering into a licensing agreement. If no authorisation is granted, they will be liable for unauthorised acts of communication to the public.

Content liability

23 When would a digital platform or online content provider be liable for mistakes in information that it publishes online? Can it avoid liability? Is it required or advised to post any notices in this regard?

Liability mostly depends on the authorship of content. Consequences for online display of wrong or inaccurate information varies depending on whether the provider's activity is subject to any industry-specific regulation (inaccurate or fake news in the case of media agents or information to consumers), that may lead to administrative offence proceedings. In such cases, liability cannot be excluded (and never in wilful intention or gross negligence) and any disclaimers or notices with such purpose would have no legal effect.

Shutdown and takedown

24 Can an internet service provider or telecommunications provider shut down a web page containing defamatory material provided by a third party without court authorisation?

Yes, ISPs may remove content or shut down web pages in the case of illegal content, regardless of the nature of the illegality, including based on defamatory material (which is a crime under Portuguese law), without a court order and regardless of a request of an interested party, provided (1) they have notice of the illegal content; and (2) they consider such illegality to be obvious, meaning that the ISP, in its reasonable opinion, finds the content to be illegal.

Under Decree law 7/2004, if the illegality is not obvious, the ISP is not obliged to remove the contested content or to prevent access to the information solely based on an interested party's claim.

INTELLECTUAL PROPERTY

Data and databases

25 Are data and databases protected by IP rights?

Yes. Electronic or non-electronic databases benefit from protection by IP rights under Decree-Law 122/2000 (transposing Directive 96/9/CE), provided they meet the originality requirement. The rights holder, unless special circumstances apply, should be the intellectual creator of such database. Databases created inside a company are presumed to be collective works and not employees' IP rights, and the patrimonial rights belong to the employer. The database manufacturer is granted a sui generis and exclusive right over the content, regardless of the structure being protected by copyright.

Third-party links and content

26 Can a website, digital platform or other online content provider link to third-party websites or platforms without permission?

Yes; however, if a third-party website or platform contains authorship rights protected work, linking or URL embedding may require the rights holder's prior consent, thus prior due diligence is a recommended practice. Content providers are advised to include legal disclaimers warning users they are exiting their environment for cybersecurity and personal data protection purposes.

27 Can a website, digital platform or other online content provider use third-party content, obtained via automated scraping or otherwise, without permission from the third-party content provider?

If such content is protected under authorship rights, prior consent by either its rights holder or a legitimate representative (eg, a collective management entity) is required.

Metaverse and online platforms

28 Are there any particular difficulties with establishing or defending copyright, database rights and trademarks on a metaverse from your jurisdiction?

There is no stand-alone definition for metaverse in Portuguese law, nor specific guidelines on IP rights on a metaverse.

Therefore, the general rules apply.

Exhaustion of rights and first-sale doctrine

29 Does your jurisdiction recognise the concept of exhaustion of rights or the first-sale doctrine? If so, how does it apply to digital products? Can rights be exhausted by placing the digital product on a metaverse or other platform in another territory?

Yes, both the Industrial Property Rights Code and the Authorship and Related Rights Code foresee the exhaustion of rights principle, as a limit to the distribution right or circulation of tangible copies, in line with Directive 2001/29/EC (InfoSoc Directive).

The implementation of the InfoSoc Directive did not result in the adoption of any policies on digital exhaustion in particular, therefore the debate on the limits of distribution of digital copies and communication to the public follows the evolution of CJEU decisions, namely the *UsedSoft* (C-128/11 – on software resale) and *Tom Cabinet* (C-263/18 – on ebooks resale) case rulings. This matter has not reached national courts.

It will be interesting to follow whether, with the evolution of the digital content market and associated technologies, notably the growth of streaming, this debate will continue to be relevant or whether it will become anachronistic or of limited applicability.

Administrative enforcement

I

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

Yes; both measures for obtaining evidence (raids) and measures for the preservation of evidence (freezing injunctions) are available, but resorting to these measures depends either on appropriate judicial proceedings before the competent court, or administrative offence proceedings before the competent authorities.

Civil remedies

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

The Intellectual Property Court is the competent judicial forum for settling civil disputes on industrial property and authorship rights. Rights holders can resort to interim and urgent measures (either to obtain or preserve evidence) or main actions on the merits (infringement of rights).

Compensation for pecuniary damages on the profit made by the infringer or loss of profit suffered by the injured party, and, in certain cases, compensation for non-pecuniary damages, can be sought.

The most sought type of remedy is the application for accessory measures (eg, temporary inhibition of the exercise of certain activities and penalty clauses).

At the plaintiff's request, the court may grant any appropriate measures to prevent imminent violations, or to prohibit a current violation of the alleged right. As a rule, these measures are granted after the defendant is notified, except where this would cause irreparable harm to the plaintiff.

In cases where the dispute is brought before the institutionalised arbitration centre competent for matters related to industrial property rights, .pt domain names, trade names and corporate names (ARBITRARE), the arbitration tribunal also has power to determine some interim or urgent measures.

DATA PROTECTION AND PRIVACY

Definition of ‘personal data’

32 How does the law in your jurisdiction define ‘personal data’? Are any other categories of personal data defined in the law? If so, what additional rules apply to the processing of such categories of personal data?

Local data protection laws do not provide additional criteria regarding these definitions compared to the ones provided for in the GDPR.

The Data Protection Act (Law 58/2019 of 8 August) does provide additional confidentiality requirements for employees, contractors and overall data processors concerning the processing of personal data concerning health.

Under Regulation No. 1/2018 of the Portuguese Data Protection Authority (CNPD), certain types of data processing activities, in addition to those provided for in article 35(3) of the GDPR, must be preceded by a data protection impact assessment (DPIA). Such types of data include, among others, data of a 'highly personal nature' using new technologies or obtained by way of novel use of existing technologies (articles 9(1) and 10 of the GDPR).

Registration and appointment of data protection officer

33 Do parties involved in the processing of personal data have to register with any regulator to process personal data? Does the law prescribe the appointment of a data protection officer?

Following the accountability principle under the GDPR, data processing activities do not require prior registration or authorisation by the CNPD, apart from exceptional cases.

In addition to the cases of mandatory appointment of data protection officers (DPOs) under article 37 of the GDPR, private entities are also required to appoint a DPO where the activity primarily carried out – either as controllers or processors – involves (1) regular and systematic monitoring of data subjects on a large scale; or (2) large-scale processing operations of special categories of data pursuant to article 9 of the GDPR or of personal data relating to criminal and administrative offence convictions pursuant to article 10 of the GDPR.

DPO appointments must be communicated to CNPD, pursuant to article 37(7) of the GDPR.

Extraterritorial issues

34 Can data protection laws and regulatory powers apply to organisations or individuals resident outside your jurisdiction? Is there a requirement for such an organisation or individual to appoint a representative in your jurisdiction?

In line with the general framework provided by the GDPR, data protection laws apply to processing operations of an establishment of a controller or a processor in the EU, regardless of whether the processing takes place in the EU or not.

In addition, the Data Protection Act (Law 58/2019) shall also apply to activities of controllers and processors not established in the EU in the cases provided for in article 3(2) of the GDPR, as well as operations:

- of an establishment situated in the national territory;
- concerning data subjects located in the national territory; and
- concerning personal data of Portuguese residents held by Portuguese consular offices abroad.

Bases for processing

35 What are the commonly asserted reasons or bases for processing personal data and for exporting or transferring personal data to another jurisdiction?

The legal bases for processing personal data and for transfer of personal data to another jurisdiction do not go beyond the GDPR (article 6), thus being mostly consent, performance of a contract, or necessary for compliance with a legal obligation to which the controller is subject.

Data export and data sovereignty

36 Are there any rules, restrictions or other relevant considerations concerning the export or transfer of personal data to another jurisdiction? Are there any data sovereignty or national security rules that require data, data servers or databases to remain in your jurisdiction?

No local particularities beyond the required level of harmonisation with the GDPR and Directive 2016/680, of 27 April 2016 (transposed by Law 59/2019), on processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, shall apply.

Sale of data to third parties

37 May a party sell or transfer personal data to third parties, such as personal data about users of an online service or digital platform?

Portugal follows closely the GDPR and general EU guidelines when it comes to personal data protection.

Portuguese law does not provide for direct restrictions to the sale or license of personal databases per se. However, in line with the GDPR rules on the lawfulness of processing, it must be ensured that both the operations of the transfer itself as well as the subsequent use of such data are executed under a valid legal basis and that, in case the sale or license implies a data transfer to countries outside the EU, such transfer is lawful under the GDPR.

Thus, the buyer's objective cannot be incompatible with the seller's original objective. Notably, in cases where the personal data was initially collected on the basis of consent, (1) data subjects must have provided specific consent for its sharing with third parties for use under a specific purpose (eg, direct marketing) and (2) such consent must have been validly collected.

Consumer redress

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?

Provisions of Chapter III (data subjects' rights) and Chapter VIII (remedies and liability) of the GDPR directly apply, and no national particularities apply. Remedies are provided to all data subjects falling under the material and territorial scope of the GDPR, regardless of citizenship.

Data subjects can also claim damages before national courts for any losses suffered from violation of data protection laws and can resort to all judicial mechanisms available.

Non-personal data

39 Does the law in your jurisdiction regulate the use of non-personal data?

No. There is no specific regulation for non-personal data, other than the right to privacy in general terms and overall confidentiality matters (including industrial or commercial/business secrecy).

DOCUMENT DIGITISATION AND RETENTION

Digitisation

40 Do the rules in your jurisdiction require any particular document or record types to be kept in original paper form and not converted solely to a digital representation?

The Portuguese government has been demonstrating an increased commitment to the multi-sectorial adoption of digital-friendly policies and procedures in the dematerialisation of relations of individuals and corporations with the public administration and in setting record-keeping obligations for compliance demonstration purposes, notably aiming to transition paper-based documentation in equivalent valid and binding alternative electronic versions, under the eIDAS Regulation.

The range of documents whose value depends solely on its original paper format is progressively decreasing. Among the most relevant cases where paper format documents are still considered to be 'originals' are the following:

- corporate and tax governance rules still require company by-laws, board decisions and tax documents to be kept in original paper form; and
- public documents issued by ministries, courts, registry offices and notaries (including notarised copies) originally issued or signed in paper versions (public deeds and powers of attorney regarding transmission of real estate) may still need to be presented on paper, namely before public entities.

Retention

41 Do the rules in your jurisdiction stipulate a minimum or maximum period for which documents or other record types should be kept?

Yes. There are multiple industry-specific document or data retention periods prescribed by statutory laws. Without prejudice to the right of keeping documentation containing personal data for performance of a contract, or based on legitimate interest (to ensure defence rights in case of litigation), under the GDPR and subject to the data minimisation principle, some of the most relevant sectorial data retention periods prescribed by law are:

- accounting records and supporting documents, including for VAT purposes: 10 years;
- contractual, preparatory and compliance documentation referring to employment relationships: five years; and
- client identification data, in case of entities subject to money laundering prevention legislation: seven years.

DATA BREACH AND CYBERSECURITY

Security measures

42 What measures must companies take to guarantee the cybersecurity of data, communications, online transactions and payment information? Does any regulation or guidance provide for a particular level of cybersecurity or specific procedures to avoid data breaches? Are there any commonly used cybersecurity standards?

All entities processing personal data must adopt the proportionate technical and organisational measures that, on a case-by-case basis, are deemed adequate to ensure data and systems security, under the general terms of article 32 of the GDPR.

Additionally, industry-specific cybersecurity requirements may apply, for example:

- critical infrastructure operators, essential services providers (financial services and digital infrastructures), digital service providers as well as any other entities using networks and information systems are also subject to Law 46/2018, of 13 August, the national legal framework on cybersecurity (transposing Directive 2016/1148 of 6 July (the NIS Directive)); and
- operators providing public communications networks or publicly available electronic communications services are also subject to the National Communications Authority's (ANACOM) Regulation 303/2019 on security and integrity of electronic communications networks and services.

The 2020 CNCS' National Cybersecurity Framework and ISO/IEC 27032, ISO 22301, ISO/IEC 22000, ISO/IEC 27000, ISO/IEC 27001 and ISO 9000 are commonly used cybersecurity standards.

Data breach notification

43 Does your jurisdiction have data breach notification laws that apply to digital business? If so, which regulators should be notified and under what conditions should affected individuals be notified?

Yes. In cases where a breach of security leads to a data breach under the GDPR, the procedures provided for in article 33(1) of the GDPR must be followed, with no applicable local law specificities. The Portuguese Data Protection Authority (CNPD) makes available an online form (in Portuguese only) that may be used for reporting breaches.

In cases where the data breach or loss of integrity occurs within certain regulated industries, additional (and, where applicable, cumulative) requirements to notification obligations apply:

- providers of publicly available electronic communications services must notify the occurrence of any personal data breaches to CNPD and, depending on the seriousness of the risks presented, to the data subjects (eg, subscribers, users, or clients);
- providers of publicly available electronic communications services or networks must notify the respective sectorial national regulatory authority (ANACOM) where the occurrence entails significant impact to the functioning of networks and services;
- entities subject to the legal framework of cyberspace security must also notify, in certain terms, incidents with serious impact on the safety of their networks and information systems or on the continuity or provision of their services, depending on the type of entity, to the National Cyber Security Centre (CNCS); and
- entities subject to financial services regulation must also report cybersecurity incidents 'likely to compromise business operations and/or threaten information security' to the Portuguese central bank (Banco de Portugal), as per Notice 21/2019. Incidents must be reported through an online portal at www.bportugal.net.

Government interception

44 Are the authorities permitted lawful access to data? If so, what types of company are required to provide data to the authorities and under what circumstances?

Under the GDPR, companies may need to process personal data (of clients, employees, users, etc) for compliance with legal obligations. Typical examples are reporting obligations to the employment and tax authorities for compliance purposes.

Other than these cases, sharing or granting access to personal data to public authorities is only lawful when expressly provided for by law and to the extent that it is necessary for the performance of a task carried out by the competent authority for the purposes of envisaged prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, or for protection of vital interests of the data subjects.

Companies are only required to share or grant access to personal data to public entities or authorities where the respective applicable legal grounds are duly demonstrated by such entities or upon a court order.

GAMING

Legality and regulation

45 Is it permissible to operate an online betting or gaming business from your jurisdiction? Is any regulatory consent or age, credit or other verification required?

Yes. Portugal has a regulated market for online games of chance and betting, whose regulator and supervisory authority is the Gambling Regulation and Inspection Authority (SRIJ). There are four different types of licences available: fixed-odds sports betting; parimutuel and fixed-odds horse racing bets; bingo; and games of chance (casino gaming and poker), and a comprehensive list of permissible and non-permissible subtypes.

Some specific online varieties are operated under an exclusive rights system by Santa Casa da Misericórdia de Lisboa (SCML) (a private charity institution of public administrative utility which traditionally holds exclusive rights for certain types of gambling) and are subject to the supervision of the social security ministry.

Engagement with these services requires prior online registration on the licensed operator's website and identity verification. Gambling is prohibited for minors (under 18 years old).

Operators cannot grant gamblers any sort of credit or loans to gamble, and gamblers cannot hold a negative credit balance with the gambling operators (ie, may not owe outstanding debts to the operators).

Cross-border gaming

46 Is it permissible to advertise, or provide access to, an online betting or gaming business located in another jurisdiction or in a metaverse?

National law is applicable to online gambling provided to customers located in Portugal even where gambling is served and hosted from places outside Portugal.

Advertising gambling services is permitted by law but only by operators licensed in Portugal and specifically targeting consumers based in Portugal. Also, advertisement campaigns are subject to restrictions on format and content and must never target or feature minors.

Although operators cannot grant users access to any other non-licensed '.pt' domain platforms, in specific cases, users may play in other duly licensed and supervised platforms, provided there is a shared liquidity agreement in place.

OUTSOURCING

Key legal issues

47 What key legal issues arise when outsourcing services to a provider either inside or outside your jurisdiction?

Regarding the internal control systems applicable to credit institutions and financial entities, regulated by Notice 3/2020 of the Bank of Portugal, special attention should be given to rules governing specific topics such as the outsourcing of operational tasks underlying the pursuance of internal control functions (which can only occur in an occasional way), and the outsourcing of the IT system to support the reporting of serious irregularities concerning its administration, accounting organisation, internal monitoring and occurrence of a breach of its obligations.

Simultaneously, EBA (EBA/GL/2019/02) and ESMA guidelines on outsourcing shall be considered.

Sector-specific issues

48 Are there any particular digital business services that cannot be outsourced or that are subject to specific regulation?

There are no specific rules.

Contractual terms

49 Does the law require any particular terms to be included in outsourcing contracts?

Under the general applicable law, no specific rules apply to contractual terms regarding outsourcing activities, despite sector-specific rules that may be imposed, depending on the scope of the contract or activities and the quality of the parties (a case-by-case analysis must be carried out).

Where the processing of personal data is included or implied within outsourcing contracts, service providers will most likely act as processors, performing data processing activities on behalf of the counterparty or controller (in which case the elements of article 28 GDPR must be included in the contract) or both parties will act as joint controllers (in which case the elements of article 26 GDPR must be included in the contract).

Credit institutions, investment firms, payment institutions and electronic money institutions subject to the supervision of the Bank of Portugal should take into due account EBA Guidelines (EBA/GL/2019/02) on outsourcing arrangements.

In labour relationships additional limitations are imposed, pursuing employees' protection.

Employee rights

50 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 in your jurisdiction?

Under new article 338º-A of the Portuguese Labour Code, it is prohibited to outsource activities that were performed by an employee whose contract was terminated in the previous 12 months by collective dismissal or individual redundancy due to the elimination of the job.

Where an outsourcing does not trigger the application of the Transfer of Undertaking (Protection of Employment) (TUPE) provisions, the employer may afterwards terminate the employment contracts of the employees who carried out the outsourced activities. The dismissal should be carried out through a redundancy procedure applicable to all employees.

This procedure (either individual or collective dismissal, depending on the number of affected employees versus the company's total headcount) is foreseen in articles 359 et seq of the Portuguese Labour Code (PLC). The procedure entails a negotiation and consultation phase with existing or created ad hoc representative structures, or with the affected employees (in case of individual redundancy). The labour authorities are present at this stage. After the consultation and negotiation are carried out, in the absence of an agreement the employer may issue the dismissal decision with 15 to 75 days' notice depending on the seniority of the employee. The dismissed employees are entitled to severance corresponding to between 12 and 14 days of salary, and seniority allowances for each year of service up to 30 April 2023 and from 1 May 2023 respectively, according to article 366 of the PLC.

ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

Rules and restrictions

51 Are there any rules, restrictions or other relevant considerations when seeking to develop or use artificial intelligence, machine learning, automated decision making or profiling? Are any particular notices of such use required? Are impact assessments recommended or required?

Other than the standard applicable framework on intellectual property law, consumer protection laws and data protection regulations, there are no country-specific statutory provisions nor relevant case law on the development or use of these types of technologies.

In cases where the technology enables decision-making solely based on automated processing of personal data, including profiling, article 22 of the GDPR shall apply.

IP rights

52 Are there any rules concerning intellectual property and artificial intelligence or machine learning? Can the training data sets and other data associated with artificial intelligence or machine learning be adequately protected by intellectual property rights? Are there particular laws, rules or guidance concerning the ownership of intellectual property created by artificial intelligence or machine learning systems?

No. To the present date, there is no local specific law nor case law in this regard. However, Portugal follows closely the European discussion on this topic (eg, the latest EPO Legal Board of Appeal decisions).

Ethics

53 Are there any rules or guidance relating to the ethics of artificial intelligence and machine learning?

Under article 9 of Law No. 27/2021 of 17 May (Portuguese Charter for Human Rights in the Digital Age), the use of artificial intelligence and robots must be guided by respect for fundamental rights, ensuring a fair balance between the principles of explainability, security, transparency, and accountability, taking into account the circumstances of each specific case and establishing processes designed to avoid any bias and forms of discrimination.

On 14 June 2023, the European Parliament adopted its final position regarding the European Artificial Intelligence Regulation proposal, which aims to regulate the development and use of artificial intelligence, ensuring that it is safe, transparent, trackable, non-discriminatory and respectful of the environment.

As at the time of writing, there is no local specific law or guideline.

TAXATION

Online sales

54 Is the sale of digital products or online services subject to taxation in your jurisdiction? If so, on what basis?

The sale of digital products or rendering of digital services is taxable in Portugal, if these are performed by a Portuguese resident company or a non-resident entity with a permanent establishment located herein, and are reflected in the company's accounting. Regarding non-resident entities' permanent establishment, it is the Portuguese tax authorities' opinion that corporate income tax may be due and tax obligations exist for entities whose servers are located in Portugal.

Server placement

55 What tax liabilities ensue from placing servers outside operators' home jurisdictions? Does the placing of servers, a platform or a metaverse within your jurisdiction by a company incorporated outside the jurisdiction expose that company to local taxes?

The Portuguese tax authorities' opinion in this regard is that a permanent establishment exists in Portugal when a non-resident entity installs a server or other physical platforms in the country. If a permanent establishment is deemed to exist in Portugal, the income derived

by such establishment should be taxable in Portugal, under both domestic legislation and the terms of double taxation treaties (as per the OECD model convention).

Electronic invoicing

56 Do the rules in your jurisdiction regulate the format or use of e-invoicing, either generally or for a specific market segment? Is there a requirement to provide copies of e-invoices to a tax authority or other agency?

The invoicing rules in Portugal do not distinguish between the type of business, market or segment, being applicable to all. Invoices in Portugal are issued electronically and must contain several elements (eg, a QR code and an ATCUD code). The invoicing programs used by resident entities must be certified by the Portuguese tax authorities and there are obligations of immediate or monthly reports of the same to the Portuguese tax authorities.

DISPUTE RESOLUTION

Venues

57 Are there any specialist courts or other venues in your jurisdiction that deal with online/digital issues and disputes?

There are no specialist courts based on the online or digital-related nature of the subject matter of a legal action per se.

However, based on the type of claim or type of service underlying the claim, the following venues may be competent for certain matters, among others (such as ADR methods), deemed relevant for online/digital business:

- The Intellectual Property Court (specialist court for IP matters), which is competent for settling disputes on authorship, industrial property rights and domain names; unfair competition and, in some cases, violation of trade secrets; and appeals against decisions of the General Inspectorate of Cultural Activities (IGAC), in administrative infringement proceedings.
- The IGAC (Inspectorate General for Cultural Activities), which has powers of control, removal and prevention of access in the digital environment to protected content and may apply administrative offence fines to intermediary networking service providers. It is also responsible for handling complaints from holders of the infringed authorship or related rights (see Decree Law 47/2023 transposing Directive 2019/790).

ADR

58 What alternative dispute resolution (ADR) methods are available for online/digital disputes? How common is ADR for online/digital disputes in your jurisdiction?

As a principle, resort to ADR methods in Portugal is done on a voluntary basis.

There are no specialist ADR methods based on the online or digital-related nature of the subject matter of a legal action. Based on the type of claim or type of service underlying the claim, cases can be dealt with through one of the following:

- consumer alternative dispute resolution entities integrated with the European Online Dispute Resolution (ODR) platform under Regulation (EU) 524/2013: competent for disputes concerning products or services bought online in the EEA;
- mediators and justices of peace, in certain cases; and
- ARBITRARE (institutionalised arbitration centre): competent for matters related to industrial property rights, .pt domain names, trade names and corporate names.

Suppliers of goods or services providers (including credit, financial and payment institutions and electronic money institutions) must inform consumers about the competent ADR centres for settling a dispute. For consumer disputes up to €5,000, resort to arbitration or mediation is mandatory, upon the consumers' express request.

UPDATE AND TRENDS

Key trends and developments

64 Are there any emerging trends or hot topics in the regulation of digital content and services, digital transformation and doing business online in your jurisdiction? Is there any pending legislation that is likely to have consequences for digital transformation and doing business online?

The past few years have seen huge momentum for technological breakthroughs, due in part to challenges relating to reliability of communications networks, and to the dematerialisation of consumer patterns, resulting in massive digitalisation of business.

This coincided with a period of revolution in the Portuguese communications paradigm, with the introduction of the fifth generation of mobile services (5G) in communications networks, as well significant proliferation of new legislation in the aftermath of the transposition (finally) of the European Electronic Communications Code and the changes in consumer protection laws (implementation of Directives 2019/771, 2019/770 and Directive 2019/2161/Omnibus), which have been ongoing since 2022.

2023, as anticipated, has been and is expected to continue to be a fruitful legislative year in these areas, mainly for consolidation of recent trends.

The implementation of the legislative package (ePrivacy Regulation, Artificial Intelligence Act, Digital Markets Act and Digital Services Act) and upcoming full entry into force will necessarily have a major impact on digital transformation and doing business online, enabling harmonisation of the legal framework throughout the EU market and the reinforcement of consumer protection and confidence, which is bound to increase growth in this sector, as well as to force companies, individuals and all interest holders to adapt their behaviours to the new reality and markets.

In respect of digital assets in the financial sector, there are two main regulations that should now be taken into consideration: (1) Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets (MiCA); and (2) Regulation (EU) 2022/858, of the European Parliament and of the Council of 30 May 2022 on a pilot regime for market infrastructures based on distributed ledger technology (DLT Regime).

On one hand, MiCA sets out a pioneering pan-European harmonised and comprehensive regulatory framework covering the issuance, offer and trading of crypto-assets and the provision of related services, which also considers the environmental impact disclosure for investors. To that extent MiCA:

- regulates the issuance and admission to trading of crypto-assets (including transparency and disclosure requirements);
- introduces licensing for crypto-asset service providers, issuers of asset-backed tokens and issuers of e-money tokens;
- clarifies regulatory obligations applicable to asset-linked token issuers, e-money token issuers and crypto-asset service providers, including consumer protection rules for the issuance, trading, exchange and custody of crypto-assets;
- strengthens confidence in crypto-asset markets by establishing a market abuse regime that prohibits market manipulation and insider trading; and
- clarifies the powers, including the framework for cooperation and sanctions, entrusted to competent authorities.

The next steps for MiCA will entail: (1) the entry into force of new requirements for stablecoins issuers (asset reference tokens, e-money tokens and overall crypto-assets issuers) by June 2024; (2) the publication of Regulatory Technical Standards (RTS) by ESMA and EBA; which will lead to (3) the entry into force of the Regulation for crypto-asset service providers (CASPs) 18 months later (by December 2024).

On the other hand, the Distributed Ledger Technology (DLT) Regime establishes the applicable requirements for DLT market infrastructures and their operators, setting out:

- the applicable requirements for existing permissions – and exemptions - to operate DLT market infrastructures;
- the requirements for mandating, modifying and withdrawing the conditions attached to exemptions and for mandating, modifying and withdrawing compensatory or corrective measures;
- the requirements for operating DLT market infrastructures;
- the requirements for supervising DLT market infrastructures; and
- the rules on the cooperation between operators of DLT market infrastructures, competent authorities and the European Supervisory Authority.

From atax standpoint, tokens and cryptocurrency are a hot topic, since Portugal enacted a personal income tax regime for income arising from cryptocurrency, which came into force on 1 January 2023. In a nutshell:

- sale of NFTs are excluded from taxation;
- gains arising from the sporadic sale of cryptocurrency are not subject to taxation if held for at least 365 days;
- nonetheless, if the trading in cryptocurrency is perceived as a business activity – due to the regularity with which it is performed – as well as mining, it will be subject to tax at the level of the individuals, at the progressive rates;
- staking will qualify as capital income and be subject, as a rule, to a flat 28 per cent rate;
- from a corporate income tax perspective, and as it happened prior to 2023, if the gains are reflected in the accounts, they should be subject to tax; and
- there will also be stamp duty charges on crypto-asset service providers.

From a labour standpoint, the alterations to the Portuguese Labour Code reflecting the government's Agenda on Dignifying Work and Valuing Young People in the Labour Market, which entered in force on 1 May 2023, include the following measures:

- creating a legal assumption of the existence of an employment contract between platforms and gig workers and between the latter and customers;
- imposing on employers a duty of information to the Labour Inspectorate, employees and their representatives, on the criteria of algorithms and artificial intelligence mechanisms used to make decisions on access to and retention of employment, as well as working conditions, including profiling and monitoring of professional activity; and
- forbidding the acquisition of third-party services to satisfy needs that have been assured by an employee whose contract terminated in the previous 12 months due to collective dismissal or redundancy, in a measure meant to prevent the replacement of employees' work with outsourcing.

Ana Rita Paínho	arp@servulo.com
Verónica Fernández	vf@servulo.com
Teresa Pala Schwalbach	tps@servulo.com
Rita Canas Da Silva	rcs@servulo.com
Ana Mira Cordeiro	ami@servulo.com

Sérvulo & Associados

Read more from this firm on Lexology