PORTUGAL

Manuel Lopes Rocha
Gonçalo Machado Borges
Magda Cocco

1. Internal Market and electronic commerce : Internet and e-commerce
1.1. Electronic Commerce, liability of Internet intermediaries

Question 1.1.1.
The Portuguese legislator transposed the E-Commerce Directive by means of Decree-Law 7/2004, of 7 January (the "E-Commerce and Data Protection Act"). In what concerns the liability of intermediary service providers, and notwithstanding the fact that Decree-Law 7/2004 has been subjected to two amendments, in 2009 and 2012, respectively, the wording of the relevant legal provisions remains the same as it did back in 2004.

During this period, some difficulties in interpreting the law have indeed been noticed, as is expected when it comes to a decade-old act that governs an ever-changing digital world.

That being said, and in what specifically concerns the definition of 'intermediary service providers', for instance, (which, one should note, is absent from the E-Commerce Directive) Portuguese courts have not strayed away from what is laid down on Article 4 of Decree-Law 7/2004 – "*'Intermediary service providers' are those that provide technical services enabling the access, provision and use of information or of online services that are independent from the very own content creation or the establishment of the services they make possible*".

As a result, the scope of 'intermediary service providers' in Portugal is quite consensual (as the Portuguese legislator put forward a definition of 'intermediary service providers', something that did not figure in the E-Commerce Directive)

although, at the same time, it is also quite broad – ISPs, web hosts, sharing websites, and others, are all taken as being 'intermediary service providers', as was envisaged by the E-Commerce Directive. Crucially, however, there is also some leeway to argue that, under Decree-Law 7/2004, social network websites, for instance, or *peer-to-peer* trackers (e.g. BitTorrent trackers, that assist in the communication between different users using the BitTorrent protocol) also act in the market vested with that quality.

It would therefore seem that the difficulties that arise out of Decree-Law 7/2004, and that involve the concept of intermediary service providers, are not intrinsically related to 'definitions' but are 'material' concerns instead. The crux of the matter is therefore what is or is not expected from intermediary service providers, as well as to who are, exactly, these intermediary service providers, bearing in mind the definition set out in Decree-Law 7/2004.

In saying this, we refer, of course, to the liability exemption provisions found in Article 13, 14 and 15 and to the correlated absence of a general monitoring obligation by intermediary service providers as laid down in Article 12 of Decree-law 7/2004, all derived from Article 12, 13, 14 and 15 of the E-Commerce Directive, respectively.

Whereas the E-Commerce Directive provided for the non-existence of a 'general obligation to monitor' in respect of providers qualifying as 'mere conduit', 'cache' and 'hosting', the Portuguese legislator instead prescribed a general exemption for all those who qualify as 'intermediary service providers', as per the definition above.

The broadness of the definition of 'intermediary service providers', as laid down on Article 4 of Decree-Law 7/2004, theoretically means that, under Portuguese law, it is possible for providers, that would otherwise not fall under the scope of Article 12, 13 and 14 ('mere conduit', 'cache' and 'hosting', respectively) of the E-Commerce Directive, to nevertheless be exempted from a duty to monitor under Portuguese law, thus making any case for their possible liability more difficult to argue (as no monitoring obligation is borne by them).

This is particularly troublesome when we bear in mind the fact that, in Portugal, as previously mentioned, one of the criteria used for establishing whether an entity is as an intermediary service provider involves an assessment of whether those technical services that are being provisioned are "*independent from the very own content creation or the establishment of services they make possible*".

In extremis, a disproportionately great number of crucial 'technical services' rendered online may be "*independent from the very own content creation*". An automated, or quasi-automated, online repository of hyperlinks and/or .torrent files, all of them uploaded by site users, could nonetheless be 'independent' from content creation or from the establishment of the services they allow for (e.g. the

download of unlawful content), and would therefore not be the subject of a general monitoring obligation.

Likewise, e-commerce hubs, social-networks, and other platforms that do play an active role over content by optimising the presentation of said content and even by imposing formal requirements over them, would also be exempted of such duty due to the fact that, ultimately, whatever role they play over that content does not preclude the fact that they are indeed "*independent from [...] content creation or the establishment of the services they make possible*".

This wording (and reading) of Portuguese law, that goes beyond what is prescribed in the E-Commerce Directive, is, naturally, troublesome, especially so in light of L'Oréal v eBay, C-324/09 (see below), as the CJEU found eBay, an online marketplace, not to be an 'intermediary service provider' because it did not take a neutral position between the customer-seller (in the sense it helps the seller promote its products and even imposes restrictions on their presentation). By placing the yardstick on a service's 'independence' from the *creation* of the end content and/or services, the provisions found on Decree-Law 7/2004, in what concerns intermediary service providers' liability may be found as being in opposition to the outcome of L'Oréal v eBay.

Question 1.1.2.

Our understanding is that, in L'Oréal v eBay, the CJEU has put forward a reasonable test for liability and has helped clarify the exact extent of the 'Hosting' defence – something of particular importance for Portugal in light of the aforementioned troublesome wording of the provisions that transpose the E-Commerce Directive.

More importantly, the CJEU's test for liability in L'Oréal v eBay has made it clear that the cornerstone of the Hosting defence is based on whether the provider has taken a neutral position between the background relationship (e.g., *in casu*, the costumer-seller relationship).

We understand that this reading of the Hosting defence may also inform all available defences under the E-Commerce Directive as well as, obviously, under all national acts that transpose said Directive.

In other words, notwithstanding the individual conditions laid down under each one of the liability exemptions found in Article 12 et seq. of the E-Commerce Directive, the underlining rationale is that, for the intermediary service provider to be exempted of liability, it shall act neutrally regarding the data provided and processed by its recipients. Therefore, as the CJEU recapped, where a service provider *"instead of confining itself to providing that service neutrally by a merely technical and automatic processing of the data provided by its customers, plays an active role of such a kind as to give it knowledge of, or control over those data*", namely by *"optimising*

the presentation of the offers for sale in question or promoting those offers", said service provider cannot be considered but a non-neutral provider, and therefore general rules on its liability shall apply.

Our take on this matter is that this line of reasoning may also be applicable to the two other defences under the E-Commerce Directive – the 'mere conduit' and 'cache' defences – insofar one properly adapts this rationale.

In other words, it is very well possible for a 'mere conduit' not to act neutrally regarding eventual unlawful acts by its consumers (only has to think of the growing number of VPN service providers that spoof consumer IPs and specifically cater to those who wish not to get caught downloading illegal content, going as far as providing complex payment mechanisms that 'whitewash' payments for using those services) and the same goes for certain caching services.

It is true that the E-Commerce Directive did bear in mind these circumstances to some extent, but in doing so emphasis was placed on 'deliberate collaboration' with service recipients in order to undertake illegal acts (see Recital 44 of the E-Commerce Directive). L'Oréal v eBay, however, seems to point out that 'malicious neglect' also will not be covered by any of the three liability exemptions found in the E-Commerce Directive. If you run a service, as an intermediary, in which you allow for, and foster (even if only indirectly) illegal acts to be undertaken by its recipients, your liability will not be exempted *per se* and it shall be assessed in light of general liability rules, regardless of whether you did have direct interference in the end contents and/or services or not.

We see this nuanced reading of the E-Commerce Directive as being paramount as an update effort under the auspices of Digital Single Market reform. We also understand that reducing the number of 'liability shields' available for intermediary service providers makes sense in light of today's concerns and the growing infiltration of the online world in everyday life. In fact, it might even help for more timely solutions regarding breaches of law without resorting to more draconian measures of control and web surveillance (as intermediary service providers will feel hard-pressed into acting quickly and responsibly upon gaining knowledge of an illegal situation).

Finally, we cannot help but refer to João Fachana's reading of how the E-Commerce Directive liability exemption regime was based in three, now arguably outdated, distinct pillars: (i) that it was unfeasible for intermediary service providers to effectively advance control over the contents uploaded and transmitter through their services; (ii) the typical neutrality of ISP's with respect to third-party contents; (iii) that an overactive liability regime could hinder internet access, propagation and, in our understanding, also e-commerce/cross-border commerce.[1]

[1] "ISP Secondary Liability – A Portuguese Perspective on Omissions as the Basis for Secondary Liability", João Fachana in Secondary Liability of Internet Service Providers, Springer, 1st ed. 2017

Indeed, it does seem that many of these pillars have been shattered or are, at the very least, trembling.

Mass data filtering technology has matured immensely during the past decade, and ISPs have abandoned their typical neutral stance towards third-party contents (one only needs to consider the net neutrality debate), and, of course, even more strikingly, the internet is pretty much everywhere these days – to the point that e-commerce has gone from underdog to a potential (and inevitable) threat to physical retail.

We therefore welcome L'Oréal v eBay's liability standard and consider that even some of its more obvious concerns have been proven groundless as time went by – no litigation thunderstorm was felt over e-commerce ever since 2011 and, ultimately, only *prima facie* liability exemption was cast aside, as the intermediary service provider's liability will still have to be established under general applicable rules (and that is enough of a challenge).

We further understand that L'Oréal v eBay, especially now alongside Stichting Brein v Ziggo, C-610/15, will have significant impact over the role (and eventual liability) intermediary service providers play in respect of the unlawful conduct of its recipients.

Question 1.1.3.

Portugal's regulation of notice-and-take down is exhausted in Decree Law 7/2004, namely in Article 18. The applicable framework, all things considered, makes for very basic regulation.

Article 18 begins by providing that intermediary service providers are not obliged to remove "contents, hyperlinks and analogous processes, or to restrict their access" only because the presumable right holder requests the provider to do so, without prejudice to the fact that said presumable right holder may nevertheless request from the relevant supervisory authority a 'preliminary decision' that shall be awarded within 48 hours and immediately made available to all intervening parties.

Said recourse to the issuing of a 'preliminary decision', however, ended up never being regulated by the Portuguese legislator (with the very own provision making itself contingent on further regulation, as per Article 18(4)). Accordingly, Portugal, in what concerns notice-and-take downs, faces a substantial legal gap in this regard.

However, in the absence of any further regulation, and bearing in mind the general obligations that nonetheless befall over intermediary service providers in accordance with Article 13 of Decree-Law 7/2004, a particularly interesting (and unique) 'self-regulated' effort has made itself noticed in Portugal. This effort, although ultimately not representing a formal notice-and-take down mechanism,

and despite being limited to copyright breaches, may be read as allowing for a procedure that is materially equivalent to notice-and-take down copyright enforcement methods.

We refer to the 30 July 2015 Memorandum of Understanding signed by the General Inspectorate for Cultural Activities ('IGAC'), the Portuguese Association of Telecommunication Operators ('APRITEL'), the Civic Movement Against Online Piracy ('MAPINET' – a group representing several copyright holders in Portugal) and the DNS.PT Association (that is in charge of registrations in the .pt top-level domain, among others,

In accordance with the Memorandum, all websites (i) holding more than 500 unauthorised copyrighted works; as well as (ii) all websites whose repositories are made up of more than 2/3 of unauthorised copyrighted material may be subjected to a DNS block, to be enacted by all Portuguese ISPs. Additionally, websites may be blocked even if they do not fulfil the aforementioned requirements should they provide access to 'particularly damaging content' (e.g., leaks, content facing authorship disputes, etc.).

The list of domains whose blocking is to be requested shall be provided for by MAPINET, alongside evidence of ongoing copyright infringement as well as evidence that MAPINET is effectively acting as an authorised proxy of the copyright holders, to IGAC. IGAC, in its turn, shall verify the information provided and subsequently notify ISPs of a decision to block said websites.

As of the date of writing, 1269 websites are currently blocked by Portuguese ISPs. This list includes pretty much all large-scale national and international websites that are/were popular unauthorised sources of copyrighted content in Portugal.

There are, however, several concerns and drawbacks to this 'para-notice-and-take down approach' that was introduced in Portugal back in 2015.

The first one is quite clear: in the absence of any further regulation on the subject-matter of Article 18 of Decree-Law 7/2004, there is no general legal framework for note-and-take down mechanisms in Portugal. This means that the solution that rose out of the 30 July 2015 Memorandum of Understanding is limited to copyright and connected rights alone. No other fast-paced, purpose-made cautionary mechanism is available for taking down hate speech, online extortion and other illegal contents online – that is still the realm of injunctions and regular legal actions.

Moreover, and perhaps more importantly, there are also significant due process and legitimacy concerns about the Memorandum of Understanding. The Memorandum of Understanding was created on an ad-hoc basis and there is no judicial supervision over the blocking of domains. In addition, IGAC has reportedly ordered the blocking of domains that were hosting lawful conduct because

of misspells at the time of identification of the domains concerned. This situation was apparently fixed on short notice.[2]

Finally, the very own technical solution used for blocking domains is fragile, at best. It works by means of a DNS blocking to outgoing requests and it can be easily evaded by using publicly-available DNS that supersedes that that is provided by ISPs to their customers. Any basic-to-intermediate user can easily change its settings within 5 minutes and gain access to websites blocked by IGAC, with no restrictions. It is, as Google's Eric Schmidt once put it, a "very simple solution to complex problems" that may ultimately backfire for all parties involved.[3]

Our opinion is that the Memorandum of Understanding, as it is, is an interesting – and welcomed – way of overcoming the absence of regulation on notice-and-take downs in Portugal. But it has its limitations. We therefore submit that the best course of action will necessarily involve further regulation on this matter, thus tackling the reason for why the very own Memorandum of Understanding came to be. The mechanism foreseen in Article 18 of Decree-Law no. 7/2004 shall be put in motion, by means of concrete regulation, and due diligence over which websites shall be blocked must be exercised. In addition, a solid appeals system – as well as an expedite mechanism of judicial supervision – shall be put in place and the scope of notice-and-take down mechanisms, in whichever form, shall extend beyond copyright enforcement. Finally, and not withstanding evident technological challenges, other more effective, non-DNS Blocking-based mechanisms shall be designed insofar there is sufficient control and accountability over their use.

Question 1.1.4.

Portuguese courts would have faced the same difficulties Belgian courts did when considering injunctions based on grounds similar to those that led to Scarlet v SABAM and SABAM v Netlog.

The legislative background behind both cases is essentially similar to that that also applies in Portugal. As mentioned before, the E-Commerce Directive was transposed in Portugal by means of Decree-Law 7/2004. In doing so, the Portuguese legislator expressly provided that no general monitoring obligation should be borne by service providers. This would mean that, in principle, when granting injunctions, national courts should ensure that their injunctions do not give rise to a 'general monitoring obligation'.

However, in both Scarlet v SABAM and SABAM v Netlog, the CJEU seems to have suggested that specific blocking requests, that are effective thereafter

[2] See https://shifter.pt/2016/01/foi-bloqueado-o-primeiro-site-nao-pirata-em-portugal/ (in Portuguese)
[3] See https://www.theguardian.com/technology/2011/may/18/google-eric-schmidt-piracy

and that do involve a seemingly mitigated general monitoring obligation, do not necessarily go against what is prescribed in the E-Commerce Directive.

As Curia's media release on Scarlet v SABAM read, "*The Court's reply is that EU law precludes an injunction made against an internet service provider requiring it to install a system for filtering all electronic communications passing via its services which applies indiscriminately to all its customers, as a preventive measure, exclusively at its expense, and for an unlimited period*". In theory, this suggests that *some* injunctions – although none of those that require measures with cumulative characteristics such as those find above – may comply with EU law, even if they do imply some sort of (mitigated) general monitoring obligation.

Recently, in 2017, the Portuguese Intellectual Property Court (a unique IP competence Court at national level) issued an injunction[4] in line with strict measures to prevent and stop the violation of IP rights spread online through a social networking service. The claim has been presented by a Portuguese Public Institute against unknown parties using its logo on TWITTER without the Claimant's authorization, using it either for wrong information or with insulting statements. The Claimant alleged that given it is an earnest public institution linked to education, with a reputation that must be defended, such inappropriate use impairs that reputation, calling into question the truthfulness of its information and the reputation that it wishes to keep.

The court decided to forbid the defendants from using such logo which is owned by the Claimant without the Claimant's authorization. At the same time the Court, at the Claimants request, ordered that TWITTER to be notified to withdraw from its messaging service all uses of the Claimant's mentioned logo that exist and are published in it. It has also been ordered to TWITTER to put in place all appropriate measures to stop and block access to the service provided by TWITTER of addresses that use the Claimant's abovementioned logo and that are not of the claimant itself.

1.2. Consumer protection in relation to the internet and E-commerce, internet purchase and contractual rights; consumer protection and dispute resolution

Question 1.2.1.

The Consumer Sales and Guarantees Directive has been implemented in Portugal by Decree-Law no. 67/2003, of 8 April, subsequently amended by Decree-Law no. 84/2008, of 21 May which introduced certain additional provisions clarifying the application of the guarantees regime to the sales of immoveable (real estate) goods. A review of judicial decisions issued in disputes concerning rights

[4] At the time this text is being written the main file is still pending.

invoked under this legal regime reveals that some issues have been repeatedly raised regarding remedies claimed by consumers.

These include questions on determining conformity of goods sold as Portuguese law has introduced a presumption of non-conformity in certain circumstances where the goods sold do not conform to objective, general, criteria rather than to contract specifications or pre-contractual information given by the seller. In these cases, determining what is the *normal quality and performance* of goods of the same type may not always be obvious and will require adducing concrete facts to support the presumption of non-conformity.

Another major issue has been determining whether consumers' rights may have lapsed by the time they initiate legal proceedings and how to assess the applicable time limits in actual cases. The issue of whether notification of defects by the consumer to the seller is made within the time limits has generated significant discussion in quite a few cases, with sellers frequently arguing that the rights asserted against them have already lapsed due to untimely notification. The summons of a seller following initiation of judicial proceedings by a consumer has already been deemed by the Supreme Court as an adequate means to give notification of no conformity, if it is effected within the two-year (for moveable goods) or five-year (for immoveable, real estate, assets) guarantee periods.

Question 1.2.2.

The proposed Directive appears to provide for appropriate rules bearing in mind the specific characteristics of digital content, its technical complexity and often intangible nature. The economic importance of activities related to digital content and the fact it can be easily, and in many cases instantaneously, purchased or accessed online by users, justify the Commission's option (reflected in Article 4) in favour of full harmonisation of the rules on digital content as the corresponding demand is growing in all Member States and a uniform set of rules will enable producers of digital content to ensure compliance throughout the EU at significantly lower costs whereas consumers will benefit from greater legal certainty.

Some aspects of the proposed Directive on digital content represent a positive effort to formulate rules that are technologically neutral and as future-proof as possible (e.g. the broad definition of digital content in Article 2(1)) whilst acknowledging that the supply of digital content has some unique features which require, for example, that interoperability with the user's devices and software be addressed when assessing conformity of the content with the contract. Other provisions may prove difficult to enforce in practice, such as the duty laid out in Article 13(2)(b) for the supplier to take all measures to avoid the use of counter-performance other than money (i.e. consumer data) following termination of the contract by the consumer.

Three innovative aspects stand out. Firstly, Article 9(1) states it is for the supplier to demonstrate conformity of content it which provides; this reversal of the burden of proof is reasonable given the technical difficulties consumers would face in demonstrating, or even detecting, the reasons for a lack of conformity, and Article 7 provides an additional safety valve for suppliers in the event of faulty integration. Secondly, by making express reference to the need for content to be free of any third party IP rights (Article 8) in order to prevent a legal defect resulting in non-conformity, the proposal should greatly minimise copyright infringement issues which are a major concern in the distribution of and access to digital content. Thirdly, Article 16 effectively outlaws binding loyalty clauses of more than 12 months in contracts for the provision of digital content by guaranteeing the consumer's right to terminate at any time following expiry of that period.

On a related note, ANACOM has recently (November 2017) issued a recommendation[5] to electronic communications operators following a significant number of complaints by mobile internet users on the billing of allegedly unsolicited content-related WAP services (e.g. ringtones, games, wallpapers). The recommendation is for operators to only bill for these services once users have expressly and specifically authorised payment for each of the contents/services by means of a durable format.

Question 1.2.3.

This proposed Directive also appears to provide for generally appropriate rules in light of its stated goal of removing contract law barriers to online trade and fully harmonising key consumer contractual rights.

Under the proposal, consumer rights are to be significantly strengthened in several respects. Determining the conformity of goods sold must take into account not only what was promised in the contract terms but also several subjective and objective criteria and incorrect installation of the goods will be deemed to constitute lack of conformity where the installation belongs to the seller's sphere of responsibilities. The reversed burden of proof for the absence of lack of conformity at the time of delivery will be extended to a period of 2 years. In addition, consumers: (i) may not be required by national laws to notify the seller of any defects, regardless of the corresponding deadlines; and (ii) must be entitled to a price reduction or to terminate the contract in situations where the seller does not repair the lack of conformity, or replace the goods purchased, within a reasonable time, even if the lack of conformity is minor.

Despite its general appropriateness in the context of online sales, this proposal risks creating two levels of protection for equivalent sale of goods transactions

[5] https://www.anacom.pt/render.jsp?contentId=1421457

depending on whether the goods are sold online or offline (according to Article 19, Directive 1999/44/EC will have its scope amended and limited to transactions which are not distance sales contracts). This may in effect make compliance more costly and complex for sellers who operate a multichannel distribution network, with traditional brick-and-mortar retail outlets alongside e-commerce platforms. Arguably, online sales will face a heavier regulatory burden with specific consumer protection rules than traditional retail of the same goods.

Question 1.2.4.
Both the proposed Directives referred to above (digital content and online and other distance sales of goods) have opted for a full harmonisation approach based on the definition of a minimum set of identical rules and an equivalent level of consumer protection in all Member States. As such, they should contribute to minimise some of the problems that currently undermine consumer protection cooperation mechanisms in the EU (e.g. traders guilty of cross-border infringements to consumer protection rules will no longer be able to evade enforcement by merely relocating to another Member State in order to benefit from more relaxed consumer protection regimes). Both Directives are to be added to the list of relevant instruments contained in the Annex to Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws. In parallel, the Commission has approved a proposal for a revised regulation on consumer protection cooperation[6] which should further contribute to effective enforcement of widespread infringements or intra-Union infringements and strengthen surveillance, alert and mutual assistance mechanisms between the competent national authorities.

Question 1.2.5.
The above instruments of EU consumer protection law already deal extensively with the main aspects that may impact on a consumer's dealings with any trader, including online sellers. The Unfair Commercial Practices Directive prohibits any unfair commercial practices, including misleading actions or omissions intended or likely to deceive consumers and aggressive commercial practices, and contains an extensive listing of types of practices which are considered unfair in any circumstances. The Unfair Contract Terms Directive introduces a general requirement of good faith that seeks to prevent significant imbalances between the rights and obligations of consumers vis-à-vis sellers and suppliers (under the corresponding legal regime in Portuguese law several unfair contract terms used by online providers have been deemed abusive and prohibited – see 1.2.6). And the

[6] COM(2016) 283 final.

Consumer Rights Directive has fully regulated aspects such as pre-contractual information to be provided to consumers, their right of (free) withdrawal in the initial stages after concluding a contract and rules on delivery conditions. These directives already protect consumers in their dealings with online platforms. Nevertheless, the fact that they have not fully harmonised national law rules on the aspects they cover has left some degree for legal fragmentation and for differing levels of protection according to each Member State. This has the potential to inhibit cross-border trade in particular regarding online sales (which are by far the main channel for distance purchases) as consumers are unsure as to exactly what rights they possess and how to exercise them depending on what platform they purchase from. In this context, the full harmonisation approach followed by the Commission in its proposals on digital content and online sales of goods seems fully justified and should adequately supplement the protection to consumers already resulting from the directives above.

Question 1.2.6.
Under the rules on standard contract terms (Decree-Law no. 446/85, of 25 October), which consumers have no possibility of negotiating, a relevant number of inhibitory actions have been brought challenging the validity of online providers' standard terms and conditions as being unfair (abusive) and seeking their prohibition. Several types of unfair clauses have been prohibited, including provisions governing the return of goods in distance contracts, liability limitations or exclusions, delivery terms and post-sales assistance to technical equipment. Traders who have been subject to these actions include online providers of consultancy services, travel and lifestyle products and retail distribution (catalogue sales). Relevant decisions, starting 2015, are published in a registry maintained by the Directorate-General for Justice Policy (DGPJ) which is available for consultation at: http://www.dgpj.mj.pt/DGPJ/sections/sobre-dgpj/anexos/registo-das-clausulas/

Question 1.2.7.
No. There do not appear to be any valid reasons why the scope of consumer protection rules should be extended to businesses and SMEs. Small and micro-businesses periodically purchase goods and services in the course of their own commercial or professional activities, or for resale, and do not warrant the same degree of protection as that which applies to consumers in B2C transactions (it is difficult to argue that any business, even an SME, is by definition a weaker party in a supply relationship). This was also the view of a majority of respondents, including consumer associations, in the context of the stakeholder consultations that preceded the proposed Directives on the supply of digital content and online and other distance sales of goods.

1.3. Geo Blocking

Question 1.3.1.

Under Regulation 1215/2012, as previously under Regulation 44/2001, in disputes arising from consumer contracts consumers are assured the benefit of opting either to sue a trader in the courts of the Member State where they are domiciled or in the courts of the Member State where the trader is domiciled (conversely, proceedings may only be brought against consumers in their own Member State). This safeguard depends, notably, on whether the trader directs commercial or professional activities to the Member State where the consumer is domiciled, condition which has been interpreted by the Court of Justice as requiring more than just having an internationally accessible website.

In joined cases C-585/08 and C-144/09, *Pammer* and *Hotel Alpenhof*, on the interpretation of Article 15(1)(c) and (3) of Regulation 44/2001, the ECJ held that determining if a trader is directing its activities to consumers in a Member State other than that of its establishment will depend on "evidence demonstrating that the trader was envisaging doing business with consumers domiciled in other Member States, including the Member State of that consumer's domicile, in the sense that it was minded to conclude a contract with those consumers" (§76). Relevant evidence may include, in addition to direct statements by the trader to the effect it is offering goods or services in one or more designated Member States, indirect factors such as: the international nature of the activity pursued; mention of telephone numbers with an international code; use of a top-level domain name other than that in which the trader is established or use of neutral top-level domain names such as '.com' or '.eu'; description of itineraries from one or more other Member States to the location where the service is provided; mention of an international clientele; or if the trader's website permits consumers to use a different language or currency to those of the trader's Member State of establishment (§§ 83, 84). In *Mühlleitner*, the Court added that factors such as the establishment of contacts or reservation of goods or services at a distance, or, *a fortiori*, the conclusion of a consumer contract at a distance, are indications of a connection between the contract and the trader's activity (case C-190/11, § 44).

In a sense, the test on "directing activities" to the Member State of the consumer's domicile rests on the degree to which a trader proactively seeks to advertise and promote its goods and services in more than its own Member State of establishment and, as such, to facilitate access by consumers residing in multiple Member States by designing its commercial activities with a wider territorial reach. In turn, the proposed geo-blocking Regulation seeks to prevent discrimination of customers (not merely consumers but also undertakings) based on geo-factors, such as nationality, place of residence or place of establishment, regardless of the format and scope with which the trader has designed its activities.

The geo-blocking Regulation will prevent traders from applying different (discriminatory) conditions of sale to consumers from different Member States in three situations set out in Article 4(1): sale of goods without physical delivery; sale of electronically supplied services; and the sale of services provided in a specific physical location. It will also prevent them from, based on the same reasons, blocking access to their websites or rerouting customers to different country versions of a website without their consent.

Although in practice compliance by traders with these obligations under the geo-blocking Regulation will sometimes coincide with factors evidencing that they direct their activities to the Member State of a consumer's domicile, under Regulation 1215/2012, each set of rules pursues different goals. The geo-blocking regulation focuses, notably, on the general conditions of sale made available by traders prior to conclusion of a contract whereas Regulation 1215/2012 relies on the test of "directing commercial activities" for jurisdictional purposes in order to ensure a more beneficial regime for consumers regarding contracts they have concluded (irrespective of their substantive terms). Furthermore, the subjective scope also differs as Regulation 1215/2012 specifies a protective jurisdictional regime for the benefit of consumers only whereas the geo-blocking Regulation extends the guarantee of non-discriminatory trading conditions to any "customers", including undertakings. Understandably, Article 1(5) of the geo-blocking Regulation expressly provides that compliance with its rules "shall not be construed as implying that a trader directs his or her activities to the Member State where the consumer has the habitual residence or domicile" within the meaning of point (c) of Article 17(1) of Regulation (EU) 1215/2012.

1.4. Questions related to the collaborative economy

Question 1.4.1

Several collaborative economy businesses have been increasing their activities in Portugal which has, predictably, generated a defensive reaction from traditional service providers.

The introduction of Uber services in Portugal, in 2014, sparked a lively debate on the regulation of passenger transport services (with a driver) and on the requirements that this type of service should be subject to in the event it is mediated by an online platform. In 2015, the Portuguese Taxi Association ("Antral") filed a legal action against Uber seeking an *ex parte* injunction to prevent the company from operating in Portugal. The injunction was granted by the first instance court and recently confirmed on appeal by the Lisbon Court of Appeals. A further appeal may lie to the Constitutional Court on constitutional issues and, in any case, serious question marks remain as to its practical effects and enforceability given that the injunction does not cover the corporate entity in the Uber

group which actually provides services in Portugal. In the meantime, the Portuguese Government has initiated a review of the regulatory framework, since it remains unclear exactly what requirements would be adequate for the provision of services by collaborative platform operators.

The short-term rental market has also been showing exponential growth, with the proliferation of Airbnb-listed houses in the main Portuguese cities leading to discussions on whether this business model should be restricted or controlled. A contentious issue, raised by recalcitrant neighbours, has been that of determining whether the provision of short-term rental services by an apartment owner, for instance, should be subject to authorisation by the building's condominium general meeting. In particular, the argument has been raised that providing short-term rental services (to the extent this constitutes a trading or commercial activity) is contrary to the residential uses provided for by urban buildings' horizontal property regulations and to each apartment's license for use (limited to residential purposes). Although, to our knowledge, Airbnb business operations have not been specifically targeted, the Lisbon Court of Appeal has already decided that the condominium general meeting must approve the conversion of residential apartments to a short-term rental business for tourists. However, this understanding was reversed by the Supreme Court in March 2017 on the grounds that even though a short-term lease, against payment by the user, may constitute an act of trade, this does not mean that a commercial activity is carried out within the leased unit as this is only made available, precisely, for residential, or accommodation, purposes.

Question 1.4.2.

Collaborative economy businesses face serious hurdles related to market access. Since they quickly become popular, this type of services has a relevant impact on traditional players. In the passenger transport sector, in particular, taxi operators complain that they must comply with stricter regulatory and licensing requirements (including quantitative restrictions on access to the market and regulated prices) which put them at a disadvantage vis-à-vis online platform operators, since the same requirements do not apply to the latter.

In December 2016, following a public consultation, the Portuguese Competition Authority ('AdC') published an extensive report on competition and regulation in passenger transport services[7] analysing the constraints that existing rules pose to competition in this market. Limitations such as quantitative restrictions on the number of operators or the administrative setting of prices (taxi tariffs are

[7] Press release available at http://www.concorrencia.pt/vEN/News_Events/Comunicados/Pages/PressRelease_2016.aspx?lst=1&Cat=2016.

set by conventions between the Directorate-General for Economic Activities and associations representing the taxi license holders) were heavily criticised by the AdC for being disproportionate and harmful to competition. As a result, the AdC recommended that the Government reassess the current quantitative restrictions and price setting regulations for taxis, with the explicit recommendation that the new rules should not extend heavy regulation to new entrants but merely establish a level playing field. The debate on regulatory reform is still ongoing.

Question 1.4.3.

The main activities in the collaborative economy in respect of which market access and licensing requirements have been the focus of discussion in Portugal are related to online platforms enabling passenger transportation services and short-term rentals for tourist accommodation.

In respect of passenger transportation services enabled by online applications, a great deal of uncertainty remains as to what market access requirements and procedures apply and, in particular, whether it is reasonable to subject this type of services to the same requirements as those applying to traditional taxi services, which are essentially contained in Decree-Law no. 251/98, of 11 August (as amended). Taxis are subject, *inter alia*, to: (i) issuance of a permit by the IMT (Institute for Mobility and Transportation), which may not be transferred and has a maximum term of 5 years; (ii) issuance of a municipal taxi license for each vehicle; (iii) quantitative restrictions, set by each municipality for at least 2-year periods, on the maximum number of taxis that may operate within each municipality.

A legislative proposal (50/XIII) by the Government was submitted to Parliament in January 2017 aiming to create a specific legal regime for "individual paid passenger transportation services in unmarked vehicles" and for online platforms enabling these services. This proposal sought to clearly distinguish transportation services offered over collaborative platforms from traditional taxi services, the former being explicitly qualified as information society services. Under this proposal, both the transportation service operators and the online platforms mediating between them and end-users would be subject only to a prior notice to the IMT. Additional conditions regarding vehicle maintenance, driver suitability and training would apply and prices would be set freely, in accordance with tariff levels or calculation formulas displayed by the platform. This proposal is still under discussion and has not been enacted.

In the case of short-term rentals, in which most residential properties on offer are made available through online platforms, the basic rules governing access to this activity are set out in Decree-Law no. 128/2014, of 29 August, which approved the legal regime on the management of short-term rental establishments. These are defined as those offering "temporary accommodation services to tourists,

for consideration, and satisfy the requirements" set out in this statute, whether accommodation is made available by physical or legal persons. Management of a short-term rental establishment is presumed to exist, *inter alia*, when an apartment or building is advertised for tourist lodging or temporary accommodation on an online platform or website.

Essentially, short-term rental providers must: a) register with the relevant municipality in their territorial area and; b) comply with sanitation and safety requirements, including fire hazard regulations. Access requirements and procedures are quite clear and transparent and registration involves a mere prior notice in an electronic platform (which must be accompanied by supporting information and documents). In addition, certain conditions specified in Administrative Order no. 83/2016, of 4 August, must be complied with, including the use of outdoor identification plates, making available a complaints book and keeping a monthly register of the number of guests.

Question 1.4.4.
In the context of collaborative economy activities, there is little visibility as to the degree or intensity of consumer complaints so far. According to the Portuguese Consumer Protection Association (DECO), although the level of complaints is still low, issues such as lack of information, non-conformity of rental properties with their online descriptions and limitations regarding protection of users' personal data have been reported.

Question 1.4.5.
According to the general definition on the scope of consumer protection rules contained in the legal regime for consumer protection (approved by Law no. 24/96, of 31 July, as amended) for a peer-to-peer provider of an underlying service to qualify as a trader it must carry out this activity in a professional capacity. Only in that case will its counterparty qualify as a consumer, as results from Article 2(1) of this statute: "A consumer is considered to be any person to whom goods are supplied, services are rendered or rights are conveyed, for non-professional use, by a person *carrying out in a professional manner an economic activity* for the obtainment of benefits." This definition fits with the definitions of a trader under Directive 2011/83/EU, for instance, or under the Unfair Commercial Practices Directive, which relies on this person's activities being carried out for purposes relating to his trade, business, craft or profession. Portuguese law does not specify when a peer-to-peer provider of an underlying service should qualify as a trader which must be assessed on a case-by-case basis. This may involve factors such as the regularity with which a person provides services or sells goods on P2P platforms (excluding merely occasional offers), revenue thresholds or what proportion of that provider's overall income is derived from these activities.

Question 1.4.6.
It is uncertain whether eventual lack of consumer confidence in peer-to-peer services requires the adoption of specific legal rules in respect of the underlying services. Consumers are generally aware that, given the flexibility and informal nature of most business models in the collaborative economy, transacting over a P2P platform may often involve a greater risk regarding the quality or fitness for purpose of the goods or services involved and may be willing to accept that risk in exchange for the advantage of lower prices or being able to purchase through sharing models. This conclusion is supported by the key findings in the exploratory study of consumer issues in online peer-to-peer platform markets published by the Commission in May 2017[8], according to which only 16% of consumers completely agreed to feeling safer or more protected when buying, renting or hiring through conventional businesses. Furthermore, the horizontal nature inherent in a peer-to-peer model (where consumer-to-consumer transactions proliferate) differs markedly from the usual "vertical" relationship between traders and consumers and in this context it may be excessive to impose specific regulation on a multitude of non-professional, mostly occasional, providers (e.g. sellers and buyers will tend to be affected by equivalent information asymmetries).

Online rating and review mechanisms are undoubtedly a useful tool to reinforce trust although, in the case of underlying service providers, this will only be effective for regular (professional) providers, who offer goods or services on multiple occasions and may, therefore, be properly rated on a minimum volume of transactions. Regarding the actual peer-to-peer platforms, accreditation mechanisms and voluntary codes of conduct may provide an additional level of safety and trust. In Portugal, the Portuguese Consumer Protection Association (DECO), together with the Digital Economy Association (ACEPI) and the DNS.PT association, have designed an accreditation mechanism that online e-commerce platforms in general may sign up to in order to benefit from a quality certification under the Confio ("Trust") stamp. They have also approved a voluntary code of conduct (Confio.pt), in accordance with Article 16 of the e-Commerce Directive, which is available at https://www.confio.pt/o-confio/codigo-de-conduta/.

2. Digital media

Question 2.1.
We have no knowledge of any national case law regarding this particular provision of the AVMS Directive and or audio-visual material offered by online newspapers.

[8] http://ec.europa.eu/newsroom/just/item-detail.cfm?&item_id=77704.

Question 2.2.
We consider that the legislative proposal to which the question refers is a step in the right direction. As regards the extension of the scope of application towards video platforms, we find that it should also cover rules on commercial communications. Portuguese law does not set out sector-specific rules for audio-visual platforms such as Youtube; however, the Law of Television establishes a legal frame-work for on-demand audio-visual services.

Question 2.3.
We have no knowledge of any disputes concerning the application of the country-of-origin principle with regard to audio-visual media service providers established in other Member States our outside the EU.

Question 2.4.
The introduction of independence requirements for media regulators at EU would, from our standpoint, be a step forward and would contribute to the creation of a single market for audio-visual media services. We are not aware of any obstacles in Portuguese law to independence requirements for media regulators; on the contrary: under Portuguese law, there are strict rules with respect to the independence of media regulators. As regards problems of undue political and or commercial pressure on media regulators in Portugal, some news arise from time to time. Yet, we are not aware of any law suits on this matter.

Question 2.5.
All the areas exemplified in the question (product placement or sponsoring; unsuitable content for minors on television; dissemination of hate speech; role of public service broadcasters; and growing media concentration) have, from time to time, been discussed in the public debate and or given cause to complaints by viewers / consumers addressed at media companies. In addition, a recent case of media concentration has been analysed (in a non-binding manner) by the Portuguese telecommunications regulator.

Question 2.6.
We are not aware of any initiatives such as those described in the question. For the time being, we do not think that an EU-wide harmonised approach is necessary.

Question 2.7.
The specific regime for copyright licencing for TV and radio broadcasting by satellite, as it results from Directive 93/83/EEC (that was transposed in Portugal by Decree-Law 333/97, of 27 November), remains relevant in Portugal, in the sense

that that regulation is still the applicable law. The Portuguese legislator, in transposing Directive 93/83/EEC, went beyond its original scope and added rules on the governing jurisdiction for disputes related to lack of authorisations by the respective right holders for retransmissions by cable. That being said, Decree-Law 333/97 was not amended ever since its entry into force in 1997.

Furthermore, and to the best of our knowledge, no Portuguese court has ever discussed the extension of the rights found in Decree-Law 333/97 to online transmissions of broadcasting organisations, nor are we are aware of any (national) discussion regarding its extension to said online transmissions.[9]

Question 2.8.

The main barriers in Portugal to cross-border portability of digital content are pretty much the same barriers that European consumers face in other Member States, meaning blocks to content and/or content that, upon being accessed, differs from the content that is made available in the respective country of residence.

However, we understand that, in what concerns Portuguese and Portuguese consumers, these barriers are made relatively more significant due to the country's peripheral position within the EU digital content market and due to Portugal's relatively smaller domestic market.

In addition, Portugal, unlike many other Member States, does not share its language with any other European country – and, unlike the situation in Denmark, Sweden and Norway (the 'Scandinavian language cluster'), language barriers and tastes in Portugal and Spain differ enough so as not to allow a one-sized approach by content providers. Thus, licensing agreements are often made separately and, more often than not, those agreements go hand-in-hand with separate localisation efforts by the respective service providers.

As a result, content that is available in Spain is often not available in Portugal – and vice-versa (although, naturally, due to different market sizes, the former occurs a lot more frequently than the latter).

Additionally, and especially in what concerns online video streams, when it is indeed possible to gain access to the same digital content across the border, localised versions of that content are often forced on customers. This means that, should a paying Portuguese consumer cross the border into Spain and be able to access the same film or TV series he/she pays for backing in Portugal, and that is also available in Spain, he/she will not have access to Portuguese subtitles and/or dubs (if applicable).

[9] In addition, the limited number Portuguese literature available on this matter mainly relates to the European Commission's consultation review of Directive 93/83/EEC and to the proposal for a regulation on ensuring the cross-border portability of online content services in the internal market.

Coincidently, and notwithstanding the fact that this much is also applicable to all other EU countries, because Portugal's only border is with Spain and because both countries exchange very significant tourism flows[10], it is not particularly surprising that cross-border portability is a significant nuisance for border-crossing Portuguese consumer. Unlike other EU consumers (e.g. Danish residents visiting Sweden or Belgians residents visiting France), Portuguese residents find a particularly adverse situation regardless of where they go, and even in their only neighbouring country.

In fact, this much is clear from the EC's Consumer Survey on cross-borders obstacles to the Digital Single Marketing, where (traveling) Portugal-based consumers constantly ranked as one of the surveyed groups that most often faced difficulties in accessing streamed online content when traveling.[11]

Ideally, these barriers should be tackled Europe-wide within the DSM strategy, thus allowing for full harmonisation of applicable rules and market access. Indeed, a fragmented legal framework on local licensing matters is what brought us here in the first place and, accordingly, the situation must be solved on a top-to-bottom basis. This is the reason why we definitely welcome Regulation (EU) 2017/1128.

The new Regulation effectively means that the monitoring of the country of residence of the consumer will cease to exist as it is today. We further understand that Regulation (EU) 2017/1128 is quite clear in relation to the (desirably) minimal role the verification of the Member State of residence shall play in the relationship at hand.

Indeed, the Regulation provides that the monitoring of the Member State of residence shall be undertaken by means of no more than two of the elements referred to in Article 1(1) and it shall be "reasonable, proportional and effective". Furthermore, in accordance with Article 8, and in is essentially a throwback to the GDPR, the use of any means to assess a country of residence shall be "limited to what is necessary and proportionate in order to achieve this purpose".

Therefore, in light of the fact that, as we interpret Article 5 of Regulation (EU) 2017/1128, service providers do not have the right – nor the obligation – to control the country of residence 'on a regular basis', and, as general rule, should

[10] Around 2 million Portuguese – out of a population of 10 million – visited Spain in 2016, and Spain has constantly ranked as the top country of origin of tourists visiting Portugal for the past 5 years. See http://rr.sapo.pt/noticia/44995/portugal_atrai_mais_turistas_espanhois_com_qualidade_e_diversidade_de_oferta *(in Portuguese)* and https://elpais.com/elpais/2017/01/31/media/1485886612_898631.html *(in Spanish)*.

[11] European Commission, Consumer survey identifying the main cross-border obstacles to the DSM and where they matter most, forthcoming 2015 – only 16% of Portuguese residents reported as being able to stream films and TV series while in another EU-country.

only do so "*at the conclusion and upon renewal of a contract*"[12], we understand any regular control of the country of residence, except where the provider "*has reasonable doubts about the subscriber's Member State of residence during the course of duration of the contract*"[13] will be unlawful, as it is not "*necessary*" nor "proportionate in order to achieve [the] purpose"[14] of Article 5.

3. Digital infrastructures

Question 3.1.

In Portugal, no formal rules on net neutrality existed prior to the adoption of Regulation (EU) 2015/2010. However, the matter in analysis was subject to two bills (418/XI/2ª, from September 30, 2010, and 103/XII/1ª, from December 3, 2011). Despite the intention to adopt the principle of net neutrality, no formal rule was approved on the matter. The only reference to this principle came with the transposition of Directive 2002/22/CE to the Portuguese legal order, with article 27, nr.1 point c) stating, in a generic way, the terms established in the above mentioned Directive[15].

In any event, the subject of net neutrality has been discussed prior to and after the adoption of this Regulation, both in the context of the civil society, events and conferences hosted by ANACOM (the country's regulator for the telecommunications sector) and in the political arena. In particular, the net neutrality subject was formally discussed in Portugal following the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions regarding "*the open internet and net neutrality in Europe*", dated April 19th, 2011.

In what concerns the practices of zero-rating, ANACOM has included the analysis and monitoring of this matter in its 2018-2020 action plan, in which ANACOM notes that it will continue to pay attention to aspects related to consumer protection, particularly those connected with the implementation of the regulation over open internet and connected to new offers by IPSs and OTT pro-

[12] See Article 5 (1) of Regulation (EU) 2017/1128.

[13] See Article 5(2) of Regulation (EU) 2017/1128.

[14] See Article 8(1) of Regulation (EU) 2017/1128.

[15] Article 27, nr.1 that "Without prejudice to other conditions provided for in general law, undertakings providing publicly available electronic communications networks and services may be subject in the exercise of their activity to the following conditions" (...) c) Transparency obligations on operators of public communications networks providing electronic communications services available to the public to ensure end-to-end connectivity, in conformity with the objectives and principles set out in article 5, disclosure regarding any conditions limiting access to and/or use of services and applications where such conditions are allowed in conformity with the law, and, where necessary and proportionate, access by the NRA to such information needed to verify the accuracy of such disclosure".

viders – including evaluation of zero rating and traffic management practices, among other related topics.

ANACOM has stated in the Report on the application of articles nr. 3 and 4 of Regulation (EU) 2015/2020 (April 2016-2017) that it is important to take into consideration the principles stated on the "BEREC Guidelines on the implementation by National Regulators of European Net Neutrality Rules", approved on August 30th, 2016.

In order to properly follow such Guidelines, ANACOM requested, in 2016, that the major Internet Service Providers ("ISP") – MEO, NOS and Vodafone – complete a survey on the zero-ratings subject, in order to acknowledge the existence (and consequent extension) of zero-ratings practices in Portugal.

ANACOM does not state, in such Report, which practices should or not be prohibited, stating only that the evaluation should be made on a case-by-case basis, and always taking into consideration the above mentioned BEREC Guidelines and any EU decision/recommendation that may be adopted in the future.

Question 3.2.

The creation of a single market for telecommunications networks or services is one of the main topics of discussion in the telecommunications sector in recent years, particularly considering the approval of Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the EU.

The idea of a pro-European approach on this matter is not new, but took a huge step forward with the Proposal for a Directive of the European Parliament and the Council establishing the European Electronic Communications Code, from September 14th, 2016 ("EECC") which establishes a general authorization mechanism for the provision of electronic communications services and networks, thus not requiring an explicit decision or administrative act by the National Regulatory Authorities ("NRA"). However, if some Member States require a notification by providers of electronic communications networks or services when they start their activities, such notification should be submitted to BEREC, which acts as a contact point and must, if necessary, forward the notifications to the NRA in all Member States in which such providers intend to provide their networks or services.

Taking this into consideration and the fact that the majority of NRAs adopt, in a great extension of their attributions, European Regulations, Directives, Decisions and Recommendations, the natural tendency may be for NRA deci-

sions and positions regarding the provision of telecommunications networks and services to become more similar and closer to each other in the underlying regulatory approach. This could contribute to the creation of a single market, including the introduction of an EU-wide licensing scheme.

However, despite the globalising nature and tendencies of the telecommunications technology and market, there are still cross-national differences in regulatory regimes, as a result of different strategic priorities, national legal outputs and the structural and commercial aspects of the market in each given EU jurisdiction.

This may act as a deterrent for a single telecommunications market in the EU. Moreover, it also important to consider the risk of a single market for telecommunications networks and services bottlenecking the activity of the service providers and jeopardizing the proper operation of NRAs as a result of centralised operations.

Moreover, specific EU initiatives aimed at unifying the EU telecom sector have been met with some opposition. This is the case, for example, of the proposed 25-year spectrum licence, which is now included on the Directive establishing the European Electronic Communications Code. Also the establishment of a pan-European licensing scheme is being met with some opposition, as NRAs are reluctant to give up control on the definition of the conditions associated with spectrum management.

In light of this, we believe that, while pan-European licencing schemes have potential in simplifying procedures and access to the activity, it is necessary to adequately determine the extent of any such licences, their scope and nature (i.e. whether they are mandatory schemes or optional). Any decision in this respect would have to take into account the various outputs of the national NRAs and the multi-faceted aspects of the telecommunications sector in the various EU Member-States.

Question 3.3.

As far as we are aware, there are currently no ongoing legal issues regarding spectrum usage and management in Portugal.

Nevertheless, in the context of its functions as regulator for the sector and as the entity responsible for ensuring the management and monitoring of an adequate and effective use of spectrum in Portugal, ANACOM has adopted strategic plans in what regards spectrum.

Specifically, ANACOM has published its 2016 Strategic Spectrum Plan, in which it identifies the main challenges associated with spectrum management in Portugal. In this context, ANACOM noted that the main priorities in this aspect are (i) the future of the 700 MHz band; (ii) mobile broadband and 5G scenario;

(iii) the timely provision of spectrum for short range communications; (iv) wireless phones and cameras; (v) IoT and M2M communications; (vi) broadband wireless communications, namely for emergency service management.

In this strategic plan, ANACOM set out the following strategic actions regarding spectrum management in Portugal:

Foster the utilization of wireless broadband technologies that allow for high speed data transmission;

Improve mobile network's coverage and capacity, namely in rural and remote areas, as well as allow for the provision of new services and mobile applications;

Develop the appropriate regulatory framework for the implementation of wireless broadband networks, by utilizing the available spectrum, such as the available frequency bands and the spectrum currently allocated for wireless broadband applications, such as in the 700 MHz, 1452-1492 MHz and 3400-3800 MHz frequency bands;Adopt the necessary measures for the provision of a total of 1200 MHz for Terrestrial Electronic Communications Services;

- Foster the growth and innovation on M2M/ IoT applications, namely by identifying and solving technical and regulatory questions;
- Evaluate the medium term needs for spectrum (until 2020) for IMT-Advanced systems, namely for LTE-A (LTE Release 10 and posterior); some of the key characteristics for IMT-Advanced systems are the provision of 100 Mbps in high mobility and 1 Gbps in low mobility, as well as increasing the efficiency of spectrum usage (bit(s(Hz); and
- Evaluate the future needs of spectrum for IMT-2020 for 5G, currently in an investigation phase, for which the first technologies are predicted to be available in 2020, being expected for these systems to reach 10 and, in some cases, 20 Gbps; In this respect it is also under investigation the provision of spectrum above 6 GHz; 5G must be seen in a wider context, involving other systems and infrastructures, such as "backhaul" systems.

ANACOM's main concerns stem directly from general legal and regulatory principles, particularly ensuring effective competition and an efficient use of spectrum, as a scarce resource.

To this effect, ANACOM carries out regular monitoring actions and has the right to ask for information and data from any provider to which rights to use spectrum have been granted. While ANACOM carries out an *ex-ante* analysis of the viability and likely effectiveness of granting a given operator the rights to use spectrum in a specific range (considering the possible use of the frequencies, its current and foreseen technological potential, the existence of other parties interested in a specific range and a possible overall impact on the market).

Ex post action is also possible and may be implemented by ANACOM through a specific administrative process, should ANACOM determine that the conditions associated with the right to use spectrum frequencies have not been complied with – this may include spectrum take-back by ANACOM.

Additionally, ANACOM has carried out several initiatives aimed at understanding the circumstances of the market and the concerns/priorities/potential associated with the various players, in order to better adjust its approach and possible action on the matter.

For example, in 2016 ANACOM conducted a public consultation regarding (i) use/availability of spectrum in the 3400-3800 MHz range. This included specific questions aimed at the desirability and potential of this spectrum range for different technologies, services and contexts. In this public consultation, ANACOM also asked for market feedback on the matter of the flexibility of the terms of use for FWA frequencies held by a major local operator.

Moreover, on 12 January 2017, ANACOM launched an applied research and development study, in the area of engineering, in order to analyse scenarios and alternative models of spectrum management, in particular those involving Licensed Shared Access (LSA) concepts in the 2.3-2.4 GHz band. The aim of this study was to evaluate whether, how and to what extent, existing systems (Program Making and Special Events – PMSE) and mobile systems could coexist in the 2.3-2.4 GHz band, taking into account the particularities of each system.

Question 3.4.

As far as we are aware, there have been no legal proceedings associated with ANACOM's independence.

4. Data in the digital economy

Question 4.1.

As is the case with all other EU State-Members, the various Portuguese stakeholders are adjusting to the upcoming reality of the General Data Protection Regulation (the GDPR).

In what concerns official initiatives towards the GDPR, the Portuguese government has established a Working Group, tasked with adjusting Portuguese legislation to the terms of the GDPR. The Working Group is composed of scholars, members of the Government, high-ranking members of the National Board of Security and of the Governmental System Management Control Centre.

In the context of its activity and attributions, the GDPR Working Group is set to work with all relevant stakeholders towards carrying out the following actions: (i) carrying out a public consultation, to take place until 30th September, 2017; (ii) identify the security rules applicable to the processing of personal data, as

per the rules in the GDPR, and present the various alternatives on institutional architecture required for operating the GDPR; and (iii) submit a law proposal by 31st December 2017.

In light of this, the GDPR Working Group has launched the public consultation on the approval of national legislation referring to the GDPR. This public consultation, which is open for input from both companies and individuals, focuses on the following 7 main topics:

1. *Processing of special categories of personal data (genetic, biometric and health data):* should specific demands be set for the processing of this data? If so, which and in what terms?
2. *Processing of data in an employment context:* should national law set specific regimes aimed at protection the rights and interests of employees in the context of labour relationships? If so, which and in what terms?
3. *Data portability rights:* should special rules be created regarding the transfer of personal data between providers of financial, banking, insurance and telecommunications services? If so, which other areas or sectors or activity should be subject to additional demands and obligations on the matter of data flows?
4. *Consent for processing of minors' personal data:* should minors under the age of 16 be allowed to expressly consent to the processing of their personal data? If so, which age should be considered as baseline: 13, 14, 15?
5. *Right to be forgotten:* should the right to be forgotten be reinforced and subject to additional guaranties in relation to what is set out in article 17 of the GDPR? If so, in which sector would that reinforcement be justified;
6. *Automated individual decision-making, including profiling:* other than the exceptions foreseen in article 22/2 of the GDPR, should other exceptions be included in respect of automated processing (namely through algorithms)? If so, in which situations?
7. *Data Protection Officer:* considering the rules in the GDPR on DPO mission and functions to be performed, would it be adequate, in certain sectors of activity, to consider the possibility of determining the appointment of specific DPOs per sector?

The public consultation is taking its course and developments are expected in the short term, with the analysis of all inputs to the public consultation from interested parties and the developments associated with the tasks entrusted to the Working Group.

Question 4.2.

As the 25th May 2018 deadline becomes a more pressing reality, businesses in Portugal are becoming increasingly aware of the impact and importance of the GDPR and of the differences between the current privacy legal framework and the one arising from this new legal instrument.

Indeed, an increasing number of companies are seeking to implement GDPR compliance programs and determining the strategic, operational and commercial impact of the GDPR on business. To this effect and by way of example, a growing number of companies are proceeding to appoint DPOs, prepare Privacy Impact Assessments for ongoing and planned data processing projects, and analysing the application of Privacy by Default and Privacy by Design Principles in the context of their activity and of the product/service at stake. This has caused a boost in the search for specialised legal services.

Moreover, stakeholders are very receptive to GDPR information, as has been noted through the various conferences, courses, seminars and various events and publications held on the matter of the overall impact of the GDPR, DPO training and awareness courses.

In what concerns the level of awareness to the GDPR by different types of stakeholders, according to a study conducted by KPMG, 65% of organizations[16] in Portugal have a medium-to-high awareness regarding the new obligations and impacts of the GDPR. However, according to this study, with less than a year remaining until the application of the GDPR, a vast majority (85%) claims to have not yet initiated the implementation process.

The public sector, the energy sector, as well as the telecommunications, transport, tourism, electronics and insurance sectors acknowledge that there is a delay regarding the implementation of the new measures arising from the GDPR. The healthcare sector and retail sector appear to have implemented measures according to the requisites of the GDPR, probably due to either regulatory constriction and/or to the fact that these sectors deal with big data and sensitive data on a regular basis. Furthermore, 53% of the inquired organizations predict a high to very high impact arising from implementation of the new measures of the GDPR and 43% claim to have designated a responsible body for the needed adaptations. In sum, in our jurisdiction there has been a gradual approach of businesses to the GDPR.

In Portugal, various entities have already begun the GDPR implementation process and are carrying out GDPR-specific compliance programs in order to review their internal procedures, policies, documents, structural organisation and overall approach to privacy and data protection compliance.

[16] More than 100 organizations of various dimensions and sectors participated in the study, which was published on March 2017.

Initially, this concern was addressed particularly by companies operating in highly-regulated sectors, such as the health and pharmaceutical sector, banking and finance, aviation and insurance sectors.

Companies in regulated sectors and/or in international groups tend to be the earlier adopters of GDPR-compliance initiatives, while small and medium-sized businesses seem to have been less quick to implement GDPR compliance programs.

Indeed, as per recent studies, out of a universe of over 1.600 small and medium-sized companies, only 3% had employed a plan towards ensuring conformity with the GDPR on 25th May, 2018; around 44% of the companies enquired admitted to not having implemented any compliance program, while 14% stated that they had employed said measures solely for specific areas[17].

However, while more robust GDPR-compliance numbers seem to be more prevalent in larger companies and companies within the context of international groups, companies operating in less regulated sectors are becoming increasingly focused on these issues, as the GDPR application comes closer to their horizon.

Question 4.3.

What are the most contentious issues in your country (from a legal viewpoint) in relation to IoT (Internet of Things) / smart cities / Machine-to-machine generated data / automated cars? (Ownership issues? Access and use? Liability in case of harm?) Are there any specific legislative measures or regulatory opinions/decisions in this area? What is the status of the policy debate?

The Portuguese Government has publicly stated its commitment to promote and implement IoT applications, smart cities and automated cars.

The market in Portugal is becoming increasingly aware of the potential of IoT, smart cities, M2M data and other corollaries of the information society. Indeed, these tools are an important asset to various market players (including banks, health and pharmaceutical companies, insurance providers and service sector providers). These entities have been investing on the development of tools and business mechanisms based on these assets and aimed at optimising resources.

Indeed, IoT is generally considered in the Portuguese market to be inevitable and a sign of the times.

An interesting side-note is that these aspects of the digital revolution have contributed to the increasing establishment of start-up tech companies, which are aimed at creating new software, hardware, business strategies and consulting services aimed at these aspects.

[17] September 2017 study by the Institute for support to small and medium companies and investment (IAPMEI) the Association for the Promotion and Development of the Information Society (APDSI) and the Portuguese Association for People Management (APG).

A common concern in this respect is the need to ensure compatibility between technological potential and user privacy/data security. Indeed, not only are data breaches an increasing reality, but the potential damage arising therefrom, particularly in regulated sectors dealing with highly sensitive information, is significant from a legal, financial and reputational point of view.

We also note that IoT may raise data ownership, spectrum, access, use and liability issues from a legal point of view. IoT devices operate as part of an ecosystem, and many of the devices are being designed to communicate with each other. As such, data ownership will continue to be an extremely important issue, as results from the EU public consultation on Building a European Data Economy which occurred between 10th of January to 26th of April 2017. Results will expectedly feed into the Commission's initiatives on data announced in the Mid-term review of the 2015 Digital Single Market strategy and contribute to a common framework on this matter.

In what concerns autonomous vehicles, Portugal is party to the Convention on Road Traffic, which permits the circulation of autonomous vehicles but not of vehicles without a driver (including one who is operating the vehicle from outside) due to the issue of control. From a legislative standpoint, the circulation of motorized vehicles on public roads depends on the existence of a human driver, placed inside the vehicle. The Government is presently pursuing the creation of tech-free zones as publicized in the 2017 state budget. As such, the main issues enunciated in the question are still being evaluated and the legal framework may be broadened and adapted to dissolve the present lack of clarification.

Question 4.4.

Although the legal right to be forgotten is not currently expressly foreseen as an independent principle in Portuguese law, it could already be taken to constitute a result of the data subject's right to object to the processing of his/her personal data, as well as the general principle that personal data may only be processed for the period of time during which it is necessary.

In practice, considering the legal emphasis on data subject protection and on the safeguard of the data subject's rights, the data subject's right to having his/her data deleted would possibly prevail over the legitimate interests of the data controller, whenever a substantially legitimate interest was not at stake. For example, data processed by employers for the purpose of managing whistleblowing programs, data pertaining to public figures in a newsworthy context or data processed by companies for the purpose of exercising legal and judicial rights would typically and generally be considered legitimate.

Note that matters associated with right of free expression and free speech, breach of privacy and other conducts which may be considered criminal offences

are handled directly by the courts, as the National Data Protection Authority ("*Comissão Nacional de Proteção de Dados*"/CNPD) only handles misdemeanours (criminal activity is reported to the State Prosecutor).

Nevertheless, we note that procedures have taken place before CNPD on this matter. In what specifically concerns the balance between data subject privacy and the search engine's commercial freedom, from May 2014 to May 2017, more than 4.300 Portuguese people officially requested Google remove search results related to their personal data (in practice, hereby exercising their right to be forgotten), with Google´s transparency report stating that 25% of these requests were complied with. As a result, 37 data subjects filed a complaint before CNPD. In this context, CNPD issued 24 decisions. According to the majority of said decisions, Google's refusals were unsubstantiated. Despite the binding nature of CNPD´s decisions, in 4 cases Google chose to proceed to court. The lawsuits are presently pending in the Lisbon Administrative Court.