XXVIII FIDE Congress

Topic 1: Internal market and digital economy

1. Internal Market and electronic commerce: Internet and e-commerce

1.1. Electronic commerce, liability of Internet intermediaries
(Stefan Kulk, Remy Chavannes)

Q1.1.1: Which difficulties (e.g. definition, delimitation) were/are your Member State and national courts confronted with when laying down rules or deciding cases where the concept of intermediary service providers is at stake?

The definition of intermediary services as provided for in Articles 12-14 of the E-Commerce Directive were essentially copied into Article 6:196c of the Dutch Civil Code ("**DCC**"). The latter provides liability exemptions for transmission, caching, and hosting of information provided by others. These liability exemptions protect intermediaries against liability for damages only. As with the E-Commerce Directive, Article 6:196c(5) of the DCC makes clear that intermediaries may still be subject to injunctions, without providing legal grounds upon which such an injunction can be based. In this regard, the question on the definition of intermediary has been primarily focussed on the liability that intermediaries may incur for damages, as opposed to the other forms of action taken against intermediaries (for instance, through injunctions). However, just as in many other EU countries, most of the controversies and court cases have been about injunctions rather than damages.

The hosting liability exemption seems to have the most practical relevance in Dutch law. In particular, it has given rise to some case law in which the scope of the exemption played a role. The exemption may apply to forums or message boards, on which users post information. However, if providers moderate or otherwise check the content that is uploaded by users, Dutch courts have held that these providers are no longer protected by the exemption because they actively engaged with the user-provided content.[1]

The CJEU made clear in both *Google France/Louis Vuitton* and *L'Oreal/Ebay* that the hosting liability exemption can also apply to non-traditional hosting service providers – service providers that do not merely store information for others but also process that information.[2] Nevertheless, the CJEU stressed that, in order to be covered by the exemption, such an intermediary must provide its services 'neutrally by a merely technical and automatic

[1] E.g. Rb. Amsterdam (vzr.) 12 March 2009, LJN BH7529; Rb. Noord-Nederland, 3 July 2013, ECLI:NL:RBNNE:2013:3992. Also see on a video-hosting platform: Rb. Amsterdam 24 November, *LJN* BP6880, par. 4.15 (Kim Holland Productions/123Video).
[2] CJEU 23 March 2010, Joined Cases C-236/08 to C-238/08, ECLI:EU:C:2010:159 (*Google France v. Louis Vuitton Malletier*); CJEU 12 July 2011, C-324/09, ECLI:EU:C:2011:474, par. 113 (*L'Oréal and others v. eBay*).

processing of the data provided by its customers.'[3] Specifically with regard to online marketplaces, the CJEU stated in *L'Oreal/Ebay* that 'the mere fact that the operator of an online marketplace stores offers for sale on its server, sets the terms of its service, is remunerated for that service and provides general information to its customers cannot have the effect of denying it the exemptions from liability.'[4]

The Dutch Court of Appeal of Leeuwarden applied the CJEU's reasoning in *L'Oreal/eBay* in a case about the Dutch online marketplace 'Marktplaats' (a subsidiary of eBay), and came to the conclusion that this service is covered by the hosting liability exemption in the DCC.[5] The fact that Marktplaats enabled its customers to promote their advertisements on the platform did not take away from that conclusion. Nor did Marktplaats' own advertisements for its platform deprive it of its status as a hosting provider.

If a service provider alters information provided by others, the service provider cannot rely on the liability exemption for hosting. Editing submitted texts and scanning and uploading photos can deprive a service provider of safe harbour protection.[6] Some uncertainty still exists with regard to certain types of algorithmic processing of information provided by others. Such processing is technical in nature, but is not necessarily 'neutral'.[7] In the *Skyscanner* case, the Dutch Court of Appeal of Amsterdam held that a flight comparison website could not rely on the liability exemption for hosting with regard to the information it collected and processed about available flights. As the website organised and ranked the information, it was 'in a way' editing the stored information.[8]

With regard to the mere conduit exemption, it is clear that it covers typical internet access providers. As to whether these intermediaries have any enduring responsibilities, such as the obligation to block particular websites, there is less certainty (see below, Q 1.1.4). There is one case that deals with the applicability of the exemption to a service provider that gave its customers access to Usenet – a newsgroup-based network that can also be used to share files.[9] Because such a provider stores information for others on its servers, the provider could not rely on the exemption for mere conduits. Instead, it was only protected by the hosting liability exemption.[10]

---

[3] CJEU 23 March 2010, Joined Cases C-236/08 to C-238/08, ECLI:EU:C:2010:159 (*Google France v. Louis Vuitton Malletier*), par. 114 and 120.
[4] CJEU 12 July 2011, C-324/09, ECLI:EU:C:2011:474, par. 113 (*L'Oréal and others v. eBay*), par. 115.
[5] Hof Leeuwarden 22 May 2012, CR, ECLI:NL:GHLEE:2012:BW6296 (*Stokke/Marktplaats*).
[6] E.g.: Rb. Haarlem 11 January 2006, ECLI:NL:RBSHE:2006:AU9504.
[7] E.g. Hof Amsterdam 7 March 2017, ECLI:NL:GHAMS:2017:739 (*Skyscanner*); and Rb. Amsterdam, 18 December 2013, available at: https://perma.cc/Z53F-4WDR. Also see: T.F.E. Tjong Tjin Tai, 'Aansprakelijkheid voor robots en algoritmes', Nederlands Tijdschrift voor Handelsrecht 2017-3, p. 123.
[8] Hof Amsterdam 7 March 2017, ECLI:NL:GHAMS:2017:739, par. 3.17 (*Skyscanner).*
[9] Hof Amsterdam, 19 August 2014, ECLI:NL:GHAMS:2014:3435 (News-Service Europe).
[10] Hof Amsterdam, 19 August 2014, ECLI:NL:GHAMS:2014:3435, par. 3.4.5 (News-Service Europe).

Q1.1.2: Do you think in L'Oréal v eBay, C-324/09, the CJEU has put forward a reasonable test for liability?

This question presupposes that the CJEU in *L'Oréal v. eBay* laid down a test for liability, when in fact the CJEU only interpreted the conditions for non-liability. Also, the broader EU law framework on intermediary liability does not lay down a test for liability. The rules in the E-Commerce Directive only negatively affect the liability of intermediaries – negative in the sense that these rules hinge on the absence, rather than the presence, of circumstances that give rise to liability.

The CJEU's decision in *eBay* is, to a large extent, a restatement the CJEU's earlier decision in *Google France v. Louis Vuitton* in which the CJEU clarified that the hosting liability exemption can apply to a search engine with regard to the advertisement space it offers.[11] In interpreting the scope of the exemption, the CJEU in *Google France* held that hosting activities should be of 'a mere technical, automatic and passive nature.' [12] To support this finding, the CJEU referred to recital 42 of the E-Commerce Directive. Strictly speaking, recital 42 of the Directive concerns only the mere conduit and caching exemptions. Although it speaks of the 'exemptions from liability established in this directive', this recital nevertheless contains a clear reference to mere conduit and caching activities.[13] Hosting is addressed in the separate recital 46. In this recital, there is no reference to 'a mere technical, automatic and passive nature'.[14] It thus seems that the CJEU in *Google France,* inadvertently or not, readjusted the scope of the hosting liability exemption.

The CJEU underlined the neutrality criterion in *eBay*, albeit in a slightly modified form. The CJEU dropped 'passive nature', and spoke only of 'merely technical and automatic processing of the data.'[15] This rephrasing of the neutrality criterion appears to bring the lack of human intervention back to the center stage. Not only are traditional, truly passive hosting providers covered by the exemption, but now intermediaries involved in the storage of information and processing thereof by algorithms and other automatic processes are also likely to benefit from the exemption. In times when intermediaries increasingly curate online information through algorithms, the nuance that *eBay* added to the applicability of hosting exemption appears to make sense.

---

[11] CJEU 23 March 2010, Joined Cases C-236/08 to C-238/08, ECLI:EU:C:2010:159 (*Google France v. Louis Vuitton Malletier*).
[12] CJEU 23 March 2010, Joined Cases C-236/08 to C-238/08, ECLI:EU:C:2010:159, par. 113 (*Google France v. Louis Vuitton Malletier*).
[13] Recital 42 of the E-Commerce Directive speaks of activities that are 'limited to the technical process of operating and giving access to a communication network over which information made available by third parties is transmitted or temporarily stored, for the sole purpose of making the transmission more efficient.'
[14] Recital 46 states that '[i]n order to benefit from a limitation of liability, the provider of an information society service, consisting of the storage of information, upon obtaining actual knowledge or awareness of illegal activities has to act expeditiously to remove or to disable access to the information concerned; the removal or disabling of access has to be undertaken in the observance of the principle of freedom of expression and of procedures established for this purpose at national level; this Directive does not affect Member States' possibility of establishing specific requirements which must be fulfilled expeditiously prior to the removal or disabling of information.'
[15] CJEU 12 July 2011, C-324/09, ECLI:EU:C:2011:474, par. 113 (*L'Oréal and others v. eBay*).

Q1.1.3: Is the regime of notice-and-take down appropriate in all kinds of situations (e.g. in cases of infringement of others' rights, such as intellectual property right, by costumers of ISSs; hate speech)? If not, what could be other appropriate solutions?

Notice-and-take down regimes lay the responsibility for finding and signalling unlawful activities on right-holders and others who are harmed by such activities. If, instead, intermediaries were to actively monitor their services, an unreasonable burden would be placed on these intermediaries that could hamper them in developing their innovative services.[16] This question presupposes that notice-and-take down is in itself an appropriate mechanism to deal with unlawful online information and activities. However, we are of the opinion that notice-and-take down mechanisms can only be appropriate if they are provided with sufficient procedural safeguards to protect against the potential chilling effects that such systems may have on freedom of expression.

The liability exemptions in the E-Commerce Directive incentivize the adoption of notice-and-take down mechanisms by intermediaries by making non-liability dependent on the absence of knowledge or awareness of illegal activities. The EU legal framework does not provide any rules on the modalities of notice-and-take down mechanisms. Rather, it leaves this to Member States who may lay down rules themselves, or who may promote self-regulatory efforts.[17] In the Netherlands, there are no formal rules regarding notice-and-take down in place. Nor does Dutch law obligate the implementation of such mechanisms. However, in one instance, a Dutch Court of Appeals ordered an intermediary to implement a notice-and-take down mechanism on the basis of Article 26d of the Dutch Copyright Act, which enables courts to issue injunctions against intermediaries whose services are used for infringements.[18]

The *Nationale Infrastructuur ter bestrijding van Cybercrime* (NICC – National Infrastructure to fight Cybercrime), the Dutch government, businesses and interest groups have created a voluntary code of conduct on 'notice and take down'.[19] This code is currently administered by ECP, which is an independent platform for businesses, Dutch government organizations, and interest groups, and aims to foster the use of information technologies in the Dutch society.[20] There is no formal list of members adhering to the code of conduct. Parties that are known by the ECP to endorse the code of conduct are listed on ECP's website.[21] For example, the code has been endorsed by internet access provider KPN, the Dutch Hosting Service Provider Association, NLKabel (an association of cable network providers), and service

[16] Moreover, such duties may be in conflict with Article 15 of the E-Commerce Directive, which prohibits general monitoring duties.
[17] Article 16(1)(a) of the E-Commerce Directive.
[18] Hof Amsterdam, 19 August 2014, ECLI:NL:GHAMS:2014:3435 (News-Service Europe).
[19] B. Koops, *Cybercrime Legislation in the Netherlands*, *in* Country report for the 18th International Congress on Comparative Law, Washington, DC, 25-31 July 2010, session "Internet Crimes" (2010), p. 31. N.A.N.M. van Eijk et al., Moving towards Balance: A study into duties of care on the Internet University of Amsterdam (2010), p. 51-52. The code is available at: http://www.ecp-epn.nl/sites/default/files/GedragscodeNTD-NL.pdf. An English version is available at: http://www.ecp-epn.nl/sites/default/files/NTD_Gedragscode_Engels.pdf.
[20] See: https://ecp.nl.
[21] For a list of endorsements, see: https://ecp.nl/activiteiten/werkgroep-notice-and-takedown.

providers such as Google and Marktplaats/eBay. In addition, Brein, which represents the entertainment industry and the anti-counterfeiting organization, SNB-react, both endorse the code. The Dutch civil liberties organization Bits of Freedom also participated in the setting up of the code of conduct,[22] but is not listed as a party that supports the code.

The code of conduct applies generally to any kind of unlawful information or conduct. It establishes a procedure for intermediaries to deal with notifications of unlawful online information. The code of conduct applies to any kind of unlawful online information or activities. This system mixes elements of notice-and-*take down* and notice-and-*notice* systems. In essence, the code requires endorsing parties to take down content when it is manifestly unlawful. If it does not consider that the materials are manifestly unlawful, the intermediary is required to inform the person that filed the notice and give an explanation. If the intermediary is not able to assess the lawfulness of the materials, the content provider is informed about the notice and requested to contact the person that filed the notice. These people then need to come to an agreement without the intermediary's involvement.[23]

In the Netherlands, there have been no noticeable attempts at the legislative level to extend the notice-and-take down regime, and to burden intermediaries with greater responsibility for unlawful activities. However, at the level of the EU, there is a clear move towards extending the responsibilities of intermediaries for user-activity. The proposed Directive on Copyright in the Digital Single Market would introduce a duty for intermediaries "that store and provide to the public access to large amounts of works" to implement content identification technologies.[24] And the proposed amendments to the Audiovisual Media Services Directive would bring 'video sharing platforms' within the domain of media regulation.[25] The amendments would give these platforms a responsibility to combat hate speech and prevent dissemination of harmful content to minors.[26] Also in other Member States, new legal duties were introduced for intermediaries that go beyond simple notice-and-take down.[27] In that sense, there seems to be a strong push on behalf of right-holder organisations to argue that notice-and-take down is no longer an appropriate means to protect the rights and interests of those harmed by online content, particularly in the domain of intellectual property and hate and harmful speech. Whether such new responsibilities are appropriate, and if they are compatible with the provisions on intermediary liability in the E-Commerce Directive, is a matter of debate.

In our view, careful attention must be paid to ensuring that a fair balance is achieved between competing fundamental rights, and to aspects of legal certainty and due process as

[22] Kamerstukken II 2003/04, 28 197, nr. 15, p. 4.
[23] Article 6 of the Code of Conduct.
[24] Commission Proposal for a Directive of the European Parliament and of the Council on Copyright in the Digital Single Market, COM 2016/593. See Article 13 of this proposal.
[25] Commission Proposal for a Directive of the European Parliament and of the Council amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services in view of changing market realities, COM(2016)287.
[26] Article 28a of the proposal.
[27] E.g.: German Bundestag, 'Bundestag beschließt Gesetz gegen strafbare Inhalte im Internet', http://www.bundestag.de/dokumente/textarchiv/2017/kw26-de-netzwerkdurchsetzungsgesetz/513398.

required by Article 52(3) of the EU Charter. In this context, useful academic work has been done to investigate the potential of creating distinct kinds of 'notice and action' measures for different kinds of potentially unlawful content (i.e. notice-and-notice for infringement of intellectual property rights, notice-wait-and-take down for defamation; and notice-and-take down, combined with occasional notice-and-suspension, for hate speech.).[28] This nuanced, compromise approach takes into account the differences in the seriousness of (alleged) interferences with fundamental rights caused by online speech, and the ease with which breaches can be verified by intermediaries.

Q1.1.4: Which difficulties were/are your Member State and national courts confronted with when considering injunctions? (Scarlet v SABAM C-70/10+ SABAM v Netlog NV C-360/10: copyright filtering injunction would create a clash with other legal principles. However, the ECJ created a checklist for specific blocking requests.)

In line with the E-Commerce Directive,[29] Article 6:196c(5) DCC leaves open the possibility of injunctions against intermediaries. It does not, however, constitute a legal grounds upon which such an injunction can be based. Injunctions can be based either on the general duty of care in Dutch tort law ("*onrechtmatige daad*", Article 6:162 DCC),[30] or other specific legal provisions. An example of such a specific provision is Article 26d of the Dutch Copyright Act, which permits courts to order intermediaries whose services are used for infringements to stop providing their service.[31] This basis for injunctions has given rise to some case law in the Netherlands. In particular, on the basis of this provision, Dutch courts have ordered hosting providers to remove websites containing copyright-infringing materials.[32] Injunctions to block access to a particular infringing website may also potentially be based on this provision. In a case about whether access providers could be ordered to block their customers from accessing the Pirate Bay website, the Dutch Supreme Court referred questions to the CJEU on whether that website was infringing and, if not, whether Article 26d might still provide sufficient legal grounds for a blocking order.[33] The CJEU recently ruled that the Pirate Bay was a directly infringing website, thereby allowing it to pass on the second question of whether (and, if so, on what grounds and under what circumstances) a national court could order access providers to block access to a website that is not infringing but which does encourage or facilitate infringement.[34]

A major difficulty with the current EU legislative framework is that it doesn't specify the conditions under which injunctions must be issued. The framework only sets the outer boundaries within which injunctions may be issued.[35] The requirements set out in the EU framework (e.g. Article 8(3) of the Copyright Directive and Articles 9 and 11 of the IP

[28] E.g. C. Angelopoulos & S. Smet (2016). 'Notice-and-fair-balance: how to reach a compromise between fundamental rights in European intermediary liability'., Journal of Media Law, 2016-8 (2), 266-301.
[29] Articles 12(3), 13(2), and 14(3) of the E Commerce Directive.
[30] E.g.: Court of Appeal Den Haag, 15 November 2010, ECLI:NL:GHSGR:2010:BO3980 (*FTD*), par. 5.9.
[31] This provision implements Article 8(3) of the Copyright Directive.
[32] E.g.: Rb. Den Haag, 17 August 2016, ECLI:NL:RBDHA:2016:9685 (*Global Layer*).
[33] HR 13 November 2015, ECLI:NL:HR:2015:3307 (*Brein/Ziggo & XS4ALL*).
[34] CJEU 14 June 2017, case C-610/15 (Brein/Ziggo).
[35] E.g.: Article 15 of the E-Commerce Directive, which prohibits general obligations to monitor; and Article 8(1) of the Copyright Directive which requires that injunctions must be "effective, proportionate and dissuasive."

Enforcement Directive) are very open and leave a lot of room for interpretation and discussion at the Member State level. Dutch legislation implementing these vague rules equally fail to add any additional conditions, procedures, limitations or safeguards that might allow for a more predictable balancing of the relevant competing fundamental rights (e.g. freedom of expression, privacy, intellectual property, freedom to conduct a business). Recent discussions before the Dutch courts on the extent to which the blocking of a website must be effective, and how that effectiveness must be assessed, are merely one example of this.[36] It remains to be seen, moreover, how the procedural safeguards demanded by the CJEU in *Telekabel Wien* as a fundamental prerequisite for any blocking measure might be implemented in practice: Dutch civil procedure does not easily enable intermediaries to test whether a particular mechanism implementing a blocking order would be sufficiently effective to avoid incurring penalties; nor does it easily allow (groups of) consumers to challenge that same mechanism for being excessively effective i.e. for also blocking legal content.

Given the absence of detail in the legislation at both EU and national level, rules on what types of injunctive relief are available, in what kinds of cases and under what conditions, must necessarily be contested in individual court cases. These are decided in first instance at Member State level, and occasionally tested by the CJEU for their compatibility with EU law, including with the fundamental rights protected in the EU Charter of Fundamental Rights. This process of finding appropriate injunctions and their modalities is a time-consuming process. The Dutch proceedings with regard to duty of access providers to block The Pirate Bay are illustrative: proceedings started in 2010 and, as of writing, have not yet come to a final conclusion.[37]

Another type of injunction that has regularly been considered by Dutch courts is the provision by intermediaries of information about customers who have allegedly used their services to disseminate unlawful content. In a landmark decision from 2005, the Dutch Supreme Court held that a hosting provider could be ordered to disclose user data if it was: (a) sufficiently likely that the hosted information was unlawful and damaging to the claimant; (b) the claimant had a sufficiently clear interest in obtaining the user data; (c) no less invasive means to obtain the user data were available; and (d) the claimant's interests outweighed those of the provider and the user.[38] Although the Supreme Court explicitly limited this rule to the issue of obtaining name and address details from hosting providers, the same criteria have subsequently been used to order the provision of other kinds of information and from other kinds of intermediaries.

One of the more pressing issues when applying these criteria, also in the light of the CJEU's decision in *Bonnier Audio*, is the extent to which the claimant demanding identifying information must provide clear evidence that the user has indeed acted unlawfully.[39] This is generally difficult for the intermediary to assess without involving the user in the

[36] HR 13 November 2015, ECLI:NL:HR:2015:3307, par. 4.3 (*Brein/Ziggo & XS4ALL*).
[37] Rb. Den Haag 11 January 2012, ECLI:NL:RBSGR:2012:BV0549, par. 1 (*Brein/Ziggo & XS4ALL*).
[38] HR 25 November 2005, ECLI:NL:HR:2005:AU4019 (Lycos/Pessers).
[39] CJEU 19 April 2012, case C-461/10, par. 56-60.

proceedings, yet Dutch civil procedure does not provide for a procedure similar to US John Doe proceedings, in which an anonymous person can appear in proceedings to defend his right to maintain anonymity.[40] An innovative approach to this conundrum was provided by the District Court of The Hague, which awarded an order to disclose user data that was suspended for two weeks to enable the user to provide a reasoned objection to the intermediary, which could then be assessed by the court. The court duly considered the user's anonymously provided objections, and ruled in the claimant's favour.[41]

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

(Marco Loos)

Q1.2.1: Which difficulties were/are your Member State and national courts confronted with when considering remedies under the Consumer Sales and Guarantees Directive?

The main difficulties lie in the question of how the remedies of repair and replacement relate to the right to termination (and price reduction). Can the consumer already terminate the contract when repair is not possible, but replacement is (or vice versa); or is the consumer then required to choose for the remedy that is available? This matter is not really addressed in case-law or literature. Secondly, it is unknown whether, in case of termination, the seller may require compensation for the loss in value of the goods that occurred during the period in which the defect had not yet manifested. If not, then the consumer may have used the goods for a long time without having to pay anything to the seller, solely because the lack of conformity did not become apparent until a later stage.[42] This is particularly relevant since under Dutch law, as opposed to the Consumer Sales Directive, a remedy for lack of conformity could arise many years after delivery, as the time limit on the right to claim a remedy is 20 years after delivery, or 2 years after notification of the defect.

Q1.2.2: Does the proposed Directive on certain aspects concerning contracts for the supply of digital content (COM(2015)634) provide for appropriate rules enabling the achievement of a genuine digital single market?

This question cannot be answered in the abstract. The proposal certainly contains good provisions, but also questionable aspects. The application of the rules to contracts for the

[40] N. Gleicher, 'John Doe Subpoenas: Toward a Consistent Legal Standard', 118 The Yale Law Journal 320.
[41] Rb. Den Haag 5 October 2015, ECLI:NL:RBDHA:2015:11408; Rb. Den Haag 6 November 2015, ECLI:NL:RBDHA:2015:12706.
[42] See M.B.M. Loos, *Consumentenkoop*, Monografieën BW B-65b, third edition, 2014, no. 37, with references.

supply of 'gratuitous' digital content are controversial, in particular as the proposal makes use of the notion of 'counter-performance' by way of the supply of personal data. While it is a good thing that such contracts are covered by the proposal, the fact that it would not apply if the information is not provided *actively* by the consumer (but instead gathered secretively through cookies by the supplier) is not to be welcomed.[43] In addition, the primacy of subjective over objective conformity criteria should be abolished,[44] and the remedies for failure to supply should be clarified (since only termination and – under very strict conditions – damages are mentioned, the question arises whether consumers may also demand specific performance).[45] The remedies for lack of conformity also need to be amended. In particular, the consequences of termination are not yet properly developed and the right to damages is too restricted without an explicit reference to national law that allows for additional possibilities to claim damages.[46]

Q1.2.3: Does the proposed Directive on certain aspects concerning contracts for the online and other distance sales of goods (COM(2015)635) and the envisaged full harmonisation of key contractual rights provide for appropriate rules enabling the achievement of a genuine digital single market?

This proposal is much more controversial. First, the limitation to online and other distance contracts is unworkable in practice. It seems therefore likely that Member States will only agree to adopt the proposal for an Online Sales Directive if its scope is enlarged to include

[43] See M.B.M. Loos, Not good but certainly content. The proposals for European harmonisation of online and distance selling of goods and the supply of digital content, in: I. Claeys and E. Terryn (eds.), *Digital contracts*, Cambridge: Intersentia, 2017, p. 3-53 (p. 29); H. Beale , Scope of application and general approach of the new rules for contracts in the digital environment, In-Depth Analysis , Briefi ng note for the Legal Aff airs Committee of the European Parliament, PE 536.493 , 2016 (available at: http://www.europarl.europa.eu/committees/nl/events-workshops.html?id=20160217CHE00181, last visited on 15 March 2017), p. 13; V. Mak , The new proposal for harmonised rules on certain aspects concerning contracts for the supply of digital content. In-depth analysis, Briefing note for the Legal Affairs Committee of the European Parliament, PE 536.495 , 2016 , (available at http://www.europarl.europa.eu/committees/nl/events-workshops.html?id=20160217CHE00181, last visited on 15 March 2017), p. 9.

[44] Beale 2016, pp. 20- 21; Mak 2016, p. 15; R. Mańko, Contracts for supply of digital content. A legal analysis of the Commission ' s directive proposal. In-depth analysis, May 2016 (available at http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_IDA(2016)582048, last visited on 15 March 2017), pp. 22-23.

[45] Loos 2017, p. 35.

[46] Loos 2017, p. 42-46; Mak 2016, p. 15; B. Fauvarque-Cosson , The new proposal for harmonised rules for certain aspects concerning contracts for the supply of digital content (termination, modification of the digital content and right to terminate long term contracts), In-Depth Analysis, Briefing note for the Legal Affairs Committee of the European Parliament, PE 536.495 , 2016 (available at: http://www.europarl.europa.eu/committees/nl/events-workshops.html?id=20160217CHE00181, last visited on 15 March 2017), p. 7.

also on- and off-premises contracts.[47] This would mean that the proposed Directive would ultimately completely replace the current Consumer Sales Directive. Secondly, the relationship between the proposal and general contract law needs to be clarified, e.g. whether consumers are entitled to damages in case of lack of conformity,[48] and whether a consumer may invoke a defect of consent, such as mistake, under national law.[49] It is a matter of policy what the period should be during which the seller is liable for lack of conformity. The original proposal to have a two-year cut off-period would decrease consumer protection as to the duration of the conformity period in one way or another in 12 Member States.[50] Moreover, from the point of view of sustainability, a longer period seems preferable.[51]

On the other hand, regarding the question of whether a defect already existed at the moment of delivery, the 2 year period during which the burden of proof is shifted (during which the seller remains liable for a lack of conformity) may prove to be too long for Member States and European Parliament.[52] However, if the proposal were to be adopted in the original form on this point, the Directive would lead to a considerable *improvement* of consumer protection in *all* Member States. This could ultimately balance out the decrease in consumer protection arising from the duration of the conformity period mentioned earlier – provided that *both* of the proposed provisions are adopted.

Q1.2.4: How do you evaluate the effect of the harmonised above rules on the enforcement of EU consumer protection legislation?

Since these Directives would replace existing national sales law and the laws applicable to digital content, Member States will not have a choice but to apply these rules to consumer contracts. Moreover, it is likely that national courts will be required to apply the implementing rules of their own motion, as is the case under the current Consumer Sales

[47] Loos 2017, p. 13-16; J.M. Smits, The new proposal for harmonised rules for the online sales or tangible goods: conformity, lack of conformity and remedies. In-depth analysis, Briefing note for the Legal Aff airs Committee of the European Parliament, PE 536,492, 2016 (available at: http://www.europarl.europa.eu/committees/nl/events-workshops.html ? id = 20160217CHE00181, last visited on 15 March 2017), pp. 7-9. See also Mańko 2016, p. 8-9, in which the at that moment mostly critical views of consumer organisations, industry associations, organisations of legal practitioners and scientists are displayed.

[48] Loos 2017, p. 18.

[49] Loos 2017, p. 18-19.

[50] Loos 2017, p. 20-21.

[51] M. Wendland, Ein neues europäisches Vertragsrecht für den Online-Handel? Die Richtlinienvorschläge der Kommission zu vertragsrechtlichen Aspekten der Bereitstellung digitaler Inhalte und des Online-Warenhandels, *EuZW* 2016, pp. 126-131 (p. 130).

[52] The Online Sales and Distance Sales Directive does not expressly deal with the consumer's right to claim damages for damage caused by the non-conformity. The Explanatory Memorandum to the proposal, p. 3, indicates that this matter is left to national law, but the text of the proposal itself gives reason to question this,

Directive[53] and will most likely be the case with regard to all Directives in the area of consumer law.[54] The proposal on goods – in particular, if it ultimately will also apply to off-line contracts – contains considerably more detailed rules than the current Consumer Sales Directive. It is therefore self-evident that more EU consumer protection legislation will be enforced by the national courts.

Q1.2.5: Do you consider that current EU consumer protection law (i.e. Unfair Commercial Practices Directive 2005/29/EC; Unfair Contract Terms Directive 1993/13/EC and Directive 2011/83/EC on Consumer Rights) appropriate for protecting consumers in their dealings with online platforms?

These Directives offer a good starting point, but leave many gaps. For instance, most of the existing consumer protection rules apply only where the trader provides goods or services in exchange for money. However, in circumstances where the consumer in fact 'pays' with other means (data or time), the contract is not covered. In addition, where the consumer is the *seller* and the trader is the buyer, again, most Directives do not apply (though the UCTD and possibly also the UCPD is/are the exception(s)). Moreover, the relationship between consumer and platforms is not well regulated (e.g. is the platform the buyer or an intermediary? How are standard contract terms incorporated? How about liabilities?). This is particularly the case when the consumer is the seller.

Q1.2.6: Has there been any action before your national courts on the basis of consumer law against online providers' terms and conditions?

Not yet, but a case between the Dutch consumer organization *Consumentenbond* and Samsung is pending.[55] Earlier, a case between a smaller consumer organization, *HCC* and Dell Computers led to the annulment of several unfair contract terms, and furthermore – since Dell ignored an order to no longer use the terms – the action ultimately to a successful claim for a *dwangsom* (French: *astreinte*).[56]

---

[53] CJEU 4 June 2015, Case C-497/13, ECLI:EU:C:2015:357 (Faber).
[54] CJEU 21 April 2016, case C-377/14, ECLI:EU:C:2016:283 (Radlinger/Finway), points 66 and 67.

[55] https://www.consumentenbond.nl/binaries/content/assets/cbhippowebsite/actie-voeren/updaten/dagvaarding-consumentenbond---samsung-11-nov-2016.pdf.
[56] Court of Appeal The Hague 6 July 2004, *NJ* 2004, 483, *TvC* 2005/4, p. 189, case note M.B.M. Loos (HCC/Dell Computer I); Court of Appeal The Hague 22 March 2005, ECLI:NL:GHSGR:2005:AT1762, *TvC* 2005/4, p. 150, case note M.Y. Schaub and M.B.M. Loos (HCC/Dell Computer II); Court of Appeal The Hague 24 October 2006, ECLI:NL:GHSGR:2006:AZ0734, *TvC* 2008/2, p. 76 (Dell Computer/HCC III).

Q1.2.7: Do you consider it necessary/useful to expand the scope of the rules on Business to Consumers (B2C) to Business to Consumers (B2B)?

Absolutely, and for several reasons. First, in contracts with other businesses, a business may still be the weaker party and in need of protection. An example relates to the terms and conditions of Internet Service Providers (ISP). These terms allow the ISP to claim full payment in case of early termination, and are frequently litigated in the Netherlands on the basis of unfair terms legislation – with differing outcomes.[57]

Secondly, since the Court of Justice defines the notion of consumer very restrictively,[58] there arise many cases where a natural person acts for dual purposes (both as a private person and in the course of a business, e.g. when buying a laptop computer) and does not fall within the protection of EU consumer law. If the scope of consumer protection rules were to be enlarged to also include such contracts, these persons would also obtain protection, and this is much needed in our opinion.[59]

1.3. Geo-blocking

(Roelien van Neck & L.E. den Butter)

Q1.3.1. The envisaged Regulation (COM(2016) aims at preventing unjustified discrimination on the basis of a consumer's domicile or nationality in cross-border situations. How do you see the interlink between this Regulation and Regulation 1215/2015 on the issue of a trader "directing activities to another Member State where the consumer has its domicile" for the purposes of determining jurisdiction?

The interlink between the Geo-blocking Regulation and Regulation 1215/2015 for the purposes of determining jurisdiction

The envisaged Geo-blocking Regulation prohibits the blocking of access to online interfaces and the rerouting of customers from one country version to another. When a trader is compliant with the Geo-blocking Regulation, its online interface will be fully and equally

[57] See Court of Appeal Arnhem-Leeuwarden, location Arnhem, 25 June 2013, ECLI:NL:GHARL:2013:4517; Court of Appeal Arnhem-Leeuwarden, location Arnhem, 4 August 2015, ECLI:NL:GHARL:2015:5803; Court of Appeal Arnhem-Leeuwarden, location Arnhem, 27 October 2015, ECLI:NL:GHARL:2015:8057; Court of Appeal Arnhem-Leeuwarden, location Arnhem, 24 May 2016, ECLI:NL:GHARL:2016:4014; Court of Appeal Arnhem-Leeuwarden, location Arnhem, 31 May 2016, ECLI:NL:GHARL:2016:4217; Court of Appeal The Hague 5 July 2016, ECLI:NL:GHDHA:2016:1845; Court of Appeal The Hague 6 September 2016, ECLI:NL:GHDHA:2016:2509; Court of Appeal Arnhem-Leeuwarden, location Arnhem, 15 November 2016, ECLI:NL:GHARL:2016:9109.

[58] CJEU 20 January 2005, case C-464/01, ECLI:EU:C:2005:32 (Gruber/Bay Wa AG).

[59] See already M.B.M. Loos, Consumer sales law in the proposal for a Consumer rights directive, *European Review of Private Law* 2010/1, p. 15-55 (p. 18-19).

accessible by customers from other Member States as well as those from the Member State to which the trader's online interface was originally addressed. The Geo-blocking Regulation stipulates that the trader may not refuse a transaction based on the domicile of customers from these Member States.[60] For the purposes of determining jurisdiction, it is relevant to determine whether this trader is now "directing its activities" to these Member States within the meaning of Article 17 (1) (c) of Regulation 1215/2012.[61]

The Geo-blocking Regulation itself answers this question as follows: the mere fact that a trader acts in accordance with the provisions of this Geo-blocking Regulation should not be construed as implying that a trader directs its activities to the relevant consumer's Member State within the meaning of Article 17 (1) of Regulation 1215/2012 (preamble par. 9-10 and Article 1 (5)). In our view, this means that when a trader is compliant with the Geo-blocking Regulation solely to fulfil its obligations under this Regulation, there is in principle no risk that Article 17 (1) (c) will be triggered (i.e. that a consumer may bring proceedings against the trader in the courts of the Member State where the consumer is domiciled).

We do, however, think that when a trader is being 'compliant plus', i.e. going further than is required under the Geo-blocking Regulation, there can be a debate whether the trader is directing its activities to the Member State where the consumer has its domicile. This is especially the case when, for example, the trader translates its website into the local language of the customer and/or offers delivery to the place of residence of the consumer, which is not required under the Geo-blocking Regulation (according to par. 18 of the preamble). We think that in such circumstances it can be assumed that this trader directs its activities to the consumer's Member State within the meaning of Article 17 (1).

For completeness, please note that in the Joined Cases Pammer (C-585/08) and Alpenhof (C-144/09) (and subsequent case-law) the European Court of Justice has given a (non-exhaustive) list of several matters that may be relevant when determining whether a trader is directing its activities to a Member State. According to the ECJ, all clear expressions of the intention to solicit the custom of that Member State's consumers could be relevant to determine whether a trader is directing its activities to a Member State.

---

[60] For further information on geo-blocking in the e-commerce sector, we would recommend reading the European Commission's findings on geo-blocking in the final report on the e-commerce sector inquiry.

[61] Articles 17 (1) (c) and 18 (1) of Regulation 1215/2012 stipulate that if a consumer contract has been concluded with a person, a trader, who pursues commercial or professional activities in the Member State of the consumer's domicile or, by any means, directs such activities to the Member State of the consumer's domicile, and the contract falls within the scope of such activities, a consumer may also bring proceedings against this party in the courts of the place where the consumer is domiciled, regardless of the domicile of the other party.

Geo-blocking and online gambling

The concept of targeting and geo-blocking is also relevant in various (regulated) sectors, including online gambling. Geo-blocking in the field of online gambling will not be prohibited under the Geo-blocking Regulation. In particular, Article 1 (3) stipulates that gambling activities are excluded from the scope of the Geo-blocking Regulation.

Until the Dutch bill on remote (online) betting and gambling comes into effect, online gambling is forbidden in the Netherlands. The Gambling Authority is targeting all online gambling operators (and also facilitators) who have a specific and distinct focus on the Dutch market. According to the Dutch Gambling Authority, this specific and distinct focus on the Dutch market can (*inter alia*) be shown by the absence of geo-blocking on Dutch customers.[62]

1.4. Questions related to the collaborative economy (COM(2016)356)

(Abe IJland)

Q1.4.1: What are the most contentious legal issues in your country raised by the collaborative economy businesses?

In the paragraph below some general legal issues presented by regulation of the collaborative economy are illustrated. The subsequent paragraph presents an example of successful cooperation between public authorities and collaborative economy businesses in the development of regulation. Competition issues are then considered under Q1.4.2, market access requirements are summarized under Q1.4.3, while Q1.4.4, Q1.4.5 and Q1.4.6 present some consumer protection issues.

Regarding the general legal issues first, a point of contention in the Netherlands has been how collaborative economy businesses should be qualified under Dutch law and whether (and to what degree) traditional sector-specific regulations, such as the Taxi Act and the Housing Act 2014, apply or should apply to them.[63] Furthermore, the liability of

[62] Factsheet enforcement with regard to online gambling (in Dutch): http://www.kansspelautoriteit.nl/publish/pages/4572/factsheet_handhaving_online.pdf.

[63] For example, one author examines the Dutch tool-sharing platform Peerby's terms of use in light of the Dutch law concept of lending and concludes that Peerby's version of lending is more akin to renting and may induce greater than anticipated liability on the part of unsuspecting 'lenders', see R. Koolhoven, 'Kwalificatie en rechtspluralisme in 'de deeleconomie'', *Maandblad voor Vermogensrecht*, nr. 6, 2015. See also the Letter of the Minister of Economic Affairs of 18 December 2015, who points out that most problems with regard to home sharing services arise from the lack of a clear distinction between private and commercial service providers, available at: https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/kamerstukken/2015/12/18/kamerbrief-over-toekomstbestendige-wetgeving-digitale-platforms-en-de-deeleconomie-waaronder-particuliere-verhuur-

collaborative economy platforms for infringements of regulations by the users of these platforms is also at issue in the Netherlands. For example, Uber has been fined as an accomplice for infringements of the Taxi Act by its drivers.[64] On the other hand, the Dutch government does not consider Uber to be a transport company, but rather an information society service provider, and as such seems to take a slightly more permissive approach to sharing economy platforms such as Uber than certain other Member States.[65]

In contrast to the legal issues presented above, some successful cooperative efforts towards regulation can certainly be noted. Examples of such cooperation are so-called 'right to challenge' experiments, in which the public authorities allow collaborative economy businesses to propose alternatives to current regulation. Amsterdam is generally regarded as progressive in its approach to the collaborative economy and has even been dubbed a 'sharing city' for its willingness to work with various collaborative economy platforms. Most notably, the city of Amsterdam entered into a Memorandum of Understanding ("**MoU**") with AirBnB, setting out common goals and rules aimed at curbing the negative effects on neighbourhoods of permanent commercial renting of apartments using AirBnB. For example, the MoU contains a rule that apartments may only be rented out for a maximum of 60 days per year.[66]

Q1.4.2: Competition issues: Does the fact that such businesses enter markets so far served by traditional service providers raise competition issues?

In the Netherlands, unfair competition concerns have been voiced — by advocates and associations for traditional service providers — that collaborative economy businesses have an unfair advantage vis-a-vis regulated traditional service providers. Some authors point out that home cooks selling meals via AirDnD for profit are not subject to inspections by the Food and Consumer Product Safety Authority, while traditional restaurant businesses are. Moreover, they point out that inhabitants who rent their apartment using AirBnB, Wimdu or Booking.com are not subject to the plethora of regulations that hotels have to comply with.

---

aan-toeristen/kamerbrief-over-toekomstbestendige-wetgeving-digitale-platforms-en-de-deeleconomie-waaronder-particuliere-verhuur-aan-toeristen.pdf

[64] CBb 8 december 2014, ECLI:NL:CBB:2014:450, 5.4.1.

[65] See Reuters newsbulletin of 25 November 2016, available at: http://www.reuters.com/article/uber-tech-spain-court/uber-in-landmark-e-u-court-battle-to-escape-strict-rules-idUSL1N1DQ0YO.

[66] Memorandum of Understanding between city of Amsterdam and AirBnB available at: https://www.amsterdam.nl/publish/pages/813509/agreement_amsterdam_and_airbnb_mou.pdf. As testimony to the success of this cooperation, the European Commission considers the MoU to be a 'best practice' in developing an EU-wide model contract for use by municipal authorities and home sharing services.

Finally, they point to ride-sharing service providers such as Uber, Lyft and BlaBlacar who are operating without a taxi license, putting licensed taxi drivers at a disadvantage.[67]

Competitions concerns related to collaborative economy businesses were addressed by a Dutch court in Uber's appeal for an injunction against enforcement of the Taxi Act's licensing requirement against Uber and its drivers in 2014. In this case, Uber argued that a ban on UberPOP served to shield the licensed taxi industry from competition and was therefore contrary to the Regulation's goals of undistorted competition in fair and open markets to increase consumer protection, freedom of choice and best value for consumers.[68] The court however ruled that the taxi licensing system was a legitimate form of market organisation and protecting licensees from unlicensed competition was inherent to such a system. [69]

Q1.4.3: <u>Market access requirements</u>: What kind of service providers active in the collaborative economy required to obtain authorisations under national law in your country and under what conditions can such authorisations be obtained? Are the relevant administrative procedures and formalities clear and transparent?

Possibly the three most relevant sets of market access requirements in the Netherlands for collaborative economy service providers are the licensing requirements for passenger transportation providers, for apartment renters and for (alcohol serving) hospitality industry operators, as they may be applicable to ride-sharing service providers, apartment-sharing service providers and meal-sharing service providers respectively.

All those who transport people by car for a reward, but not as public transport, are required to obtain a taxi license under the Taxi Act. The requirements for a taxi license are contained in the Passenger Transport Decree 2000, and include a requirement of trustworthiness (to be demonstrated by a so-called declaration of good behaviour) as well as a requirement of skill (to be demonstrated by the completion of training for taxi drivers).

Second, a license is required to be able to use apartments with a permanent housing designation for purposes other than housing, such as renting them out for use as tourist accommodations. The Housing Act 2014 prohibits taking apartments — in buildings designated as housing — out of the 'housing supply' by using it for other purposes than permanent residence without a license from the city council. For example, the city of Amsterdam has designated most apartments as housing and has a broad discretion to refuse

[67] S. Ranchordas 2016, 'regels voor de digitale deeleconomie, oftewel 'uber-regulering', RegelMaat, 2016 (2).
[68] CBb 8 december 2014, ECLI:NL:CBB:2014:450, 5.7.
[69] CBb 8 december 2014, ECLI:NL:CBB:2014:450, 5.7.1.

licenses which take apartments out of the housing supply. Enforcement of this licensing requirement has resulted in fines for homeowners who are held responsible for the renting of their apartments on AirBnB, even if their tenants were sub-letting the apartment.[70]

Finally, a license is required to serve drinks in a venue by trade or as a business according to the Licensing and Catering Act 2013. The requirements for a license to operate a hospitality business are contained in the Licensing and Catering Decree, and include *inter alia* requirements concerning the 'social hygiene' of the venue and of persons in charge of the venue as well as a screening of the applicant for the potential danger of use of the venue for money laundering or other criminal acts under the Public Administration Probity Screening Act.

Q1.4.4: Consumer protection[71]: Are consumer protection issues the subject of legal challenges in your country?

To the knowledge of the authors, no challenges to collaborative economy businesses have been mounted by consumers based directly on consumer protection provisions. Consumer protection considerations were however at the core of Uber's appeal for an injunction against enforcement of the Taxi Act's licensing requirement against it and its drivers in 2014.[72] In short, Uber argued that its requirements for drivers guaranteed a sufficient level of consumer protection; so that application of the licensing requirement under the Taxi Act would not be necessary to guarantee the necessary level of protection for its customers. The court however ruled that the fact that a recent bill of health and a specific taxi driver's training course are required in order to obtain a license under the Taxi Act meant that Uber's requirements were not substitutable for the requirements under the Taxi Act.[73] Furthermore, the court ruled that the level of enforcement by Uber of its policies was not up to par with the public enforcement of the licensing requirements, and could therefore not be substituted for public oversight.[74]

Q1.4.5: Under which conditions in a peer-to-peer provision of services the provider of the underlying service qualifies as a trader according to your national law?

[70] ECLI:NL:RVS:2017:649.
[71] "*EU consumer law applies to any collaborative platform that qualifies as a 'trader' and engages in 'commercial practices' vis-à-vis consumers. Conversely, EU consumer and marketing legislation does not apply to consumer-to-consumer transactions.*"
[72] ECLI:NL:CBB:2014:450.
[73] ECLI:NL:CBB:2014:450, para. 5.6.4.
[74] Ibid.

The definition of a trader is any natural or legal person who is acting for purposes relating to his trade, business, craft or profession and anyone acting in the name of or on behalf of a trader. The Dutch Civil Code ("**DCC**") actually contains several, albeit similar, definitions of a trader in provisions implementing the different EU Directives for consumer protection. The Consumer Protection Enforcement Act refers to traders as mentioned in:

(i) Directive 2005/29/EC on Unfair Commercial Practices (implemented in section 3A of title 3 of book 6 DCC),
(ii) Directive 2011/83/EU on Consumer Rights (implemented in section 2B of title 5 of book 6 DCC),
(iii) Timeshare Directive 2008/122/EC (implemented in title 1A of book 7 DCC).

The Dutch Government has acknowledged that the frequency of trading, an aim of generating profits and the size of turnover can be criteria to determine whether someone is acting in the capacity of a trader. However, it also warns that the legal definition of a trader should not be unduly limited, and therefore other circumstances may have to be considered on a case-by-case basis. In the same vein, it has acknowledged that it may be difficult to establish thresholds based on generated income, in deciding whether an activity is performed by a trader or not, without considering the particular features and legal context of the market in which the activity at issue is performed.[75] In this regard, see also the answer to Q1.2.7 above.

Q1.4.6: How can legal rules contribute to remedying the lack of consumer confidence in peer-to-peer services? Do you think that trust-building mechanisms such as online rating and review systems and quality labels are appropriate tools to overcome the lack of information about individual service providers? What other tools would you consider appropriate?

A recent study commissioned by the Dutch government on the opportunities and obstacles for innovation in the sharing economy recognizes the value of review systems, and even hints at a role for the government to manage a central review system in order to avoid lock-

[75] Letter of the Minister for Foreign Affairs of 8 July 2016, TK 2015-2016, 22112, nr. 2172, available at: https://www.eerstekamer.nl/behandeling/20160708/brief_regering_fiche_een_europese/document3/f=/vk5posimhzzg.pdf.

in effects caused by the fact that reputations are usually non-transferable from one platform to another.[76]

2 Digital Media
Lucky Belder & Stijn van Deursen

Q2.1: In its judgment of 21 October 2015 in *New Media Online GmbH v Bundeskommunikationssenat* (case C-347/14), the CJEU held that the concept of 'programme', within the meaning of Article 1(1)(b) of the AVMS Directive, must be interpreted as including, under the subdomain of a website of a newspaper, the provision of videos of short duration consisting of local news bulletins, sports and entertainment clips. It held that online newspapers are not per se excluded from the scope of the AVMSD. If publishers offer audio-visual material they may be covered by the Directive, provided that the principal purpose test is met.
Is your national practice in line with this judgment? If not, where does (or did) it deviate? Did the judgment of the CJEU lead to a different approach in your country?

According to Article 1.1 of the Dutch Media Act, a *programme* ('programma') is an electronic product with visual or media content, that is clearly recognisable and broadcasted as such under a distinctive title via a broadcasting service ('omroepdienst'). A *broadcasting service* ('omroepdienst') is defined as a media service ('mediadienst') that provides media content on the basis of a chronological schedule, which is determined by the institution responsible for the media content, whether or not encrypted by means of a broadcasting channel or broadcasting network, and distributed for simultaneous reception by the general public or a part of the general public. A *media service* is a service that provides media content via public electronic communication networks, for which the supplier has editorial responsibility. As follows from the foregoing, to be qualified as a programme, it is required that the media content is distributed via a broadcasting service, and that the content is received simultaneously by the general public or a part of it. Therefore, according to Dutch law, videos as defined in the judgement would not qualify as a programme. They would however qualify as a media service (on-demand) and therefore fall within the scope of regulation. Since the result of this classification will be that audio-visual material is covered by the Directive and will therefore be governed by the same set of rules, the judgement has not lead to a different approach and will presumably not do so.

[76] ShareNL, 'Innoveren in de deeleconomie', 2015, p. 24-25, available at: https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2015/11/01/innoveren-in-de-deeleconomie/innoveren-in-de-deeleconomie.pdf.

Q2.2: The legislative proposal to amend the AVMS directive brings video platforms (such as YouTube) under the scope of the AVMS rules. Do you consider this a step in the right direction? How far should the extension of the scope of application towards such platforms go: only for the rules on protection of minors and the combatting of hate speech, or also for the rules on commercial communications (product placement, sponsoring, advertising…)? Does your national legislation already provide for sector-specific rules for audio-visual platforms?

In the light of the increasing importance of video platforms, resulting in convergence with traditional media, and the role that these platforms play in society, bringing video platforms under the scope of the AVMS may be considered a necessary next step.

Under Dutch legislation, only media services are regulated. A key element in the definition of media services is editorial responsibility. The concept of editorial responsibility is defined in Article 1.1 Dutch Media Act 2008. According to this definition, editorial responsibility means effective control over the choice of media content and the organisation of the media content in a chronological schedule (for programmes) or in a catalogue (for media services on-demand). As most video platforms do not work within such a system of editorial responsibility, they are not regulated.

However, if a system of editorial responsibility does apply, a video platform will be considered a media service on-demand ('commerciële mediadienst op aanvraag') and will therefore be regulated by the applicable provisions in the Dutch Media Act 2008. This includes rules on product placement and the protection of minors against harmful content. In Dutch legislation there are no sector-specific rules for audio-visual platforms. One of the priorities of the Dutch Media Authority in 2017 is the online domain and new ways of access to media content. Therefore, the Dutch Media Authority will focus on the registration on media services on-demand, protection of minors against (seriously) harmful content ('ernstige schade'), surreptitious audio-visual commercial communication ('sluikreclame'), unlawful product placement and other forms of hidden commercial influencing.[77] Moreover, the Dutch Media Authority advocates the regulation of online media in the new AVMS Directive and, until this Directive is implemented in Dutch legislation, is seeking to stimulate initiatives of self-regulation in the online field. .Nonetheless, at this time, there are no sector-specific rules under Dutch legislation.

Q2.3: One of the major areas of debate in the context of the AVMS revision, concerns the country-of-origin principle and the criteria for jurisdiction. Have there been any disputes in your country concerning the application of the country-of-origin principle (whereby the media regulator attempted to impose certain rules on audio-visual media service

[77] Commissariaat voor de Media, 'Toezichtbrief 2017: Het nieuwe kijken en het huis op orde', para. 9-14, . 24 November 2016.

providers established in other Member States)? Have there been any problems regarding providers established outside the EU and targeting your national audience?

Before answering this question, we would like to refer to the jurisprudence developed in the eighties regarding the Netherlands and its regulation of advertising in broadcasts from other countries. In Case 352/85 (Bond van Adverteerders), the CJEU ruled that the act of broadcasting from one country to the national audience of another country constitutes a transnational service, involving both the service of broadcasting and the service of advertising and that national barriers may only apply — without interfering with the freedom of providing services — under strict conditions. In Case 353/89 (Commission v. Netherlands) it was pointed out that certain conditions on the broadcasting of advertising in television programs from other states may infringe the freedom of providing services in the Treaty.[78]

In the Netherlands, jurisdiction over broadcasts from other countries is regulated by Article 1.2 Dutch Media Act 2008, referring to Article 2 AVMS. Disputes concerning the jurisdiction of the Dutch Media Authority arose in 2001[79] and 2003[80] and, therefore, under the "Television without Frontiers" Directive 98/552/EEC .[81]

Both decisions concerned a dispute between the Dutch Media Authority and HMG, that broadcasts the Dutch TV-channels RTL4 and RTL5. The official seat of HMG was in Luxembourg, the editorial policy decisions of the board of directors were taken in Luxembourg and RTL4 and RTL5 were being broadcast under a Luxembourg license. On the basis of Article 2 of the Television without Frontiers Directive ("the Directive"), the Dutch Media Authority nevertheless considered that it had jurisdiction over the TV-channels as they fell within the scope of the Dutch Media Act. According to the Dutch Media Authority, HMG was the broadcasting organisation that was responsible for the broadcasting of the channels and, since it had its centre of activities in the Netherlands, most of the HMG-staff involved in the TV-activities were based in the Netherlands. Furthermore, the actual editorial decisions were taken in the Netherlands. Moreover, most of the HMG personnel involved in the pursuit of television activities were based in the Netherlands. Therefore, according to the Media Authority, the provisions of the Dutch Media Act would apply to *RTL4* and *RTL5*.

In its 2001-decision, the highest Dutch administrative court ruled that the Dutch Media Authority was right to assume jurisdiction. However, this would result in double jurisdiction, since the Luxembourg Media Authority also claimed jurisdiction in

[78] ECJ, 26 April 1988, C-352/85 (Bond van Adverteerders), 26 April 1988; C-353/89, Commission v. The Netherlands, 25 July 1991.
[79] ABRvS 10 april 2001, ECLI:NL:RVS:2001:AB1451, *Mediaforum* 2001-6, nr. 27.
[80] ABRvS 6 augustus 2003, ECLI:NL:RVS:2003:AI0788, *Mediaforum* 2003-9, nr. 44.
[81] Both cases are dated before the AVMS, The earlier Directive 89/552/EEG first regulated the country of origin in Article 2.

circumstances where the Dutch Media Authority did not sufficiently comply with its obligation to prevent such cross-overs. Therefore the court overruled the decision.

In 2002, the Dutch Media Authority claimed jurisdiction again, after having discussed the topic in the Contact Committee. However, Luxembourg did not want to give up jurisdiction and the case was brought to court again. The court annulled the decision of the Dutch Media Authority in 2003 on the grounds that it would not be compliant with the Directive and the principle of loyalty as laid down in Article 10 EC regarding compliance with the objectives, system and aim of the Treaty and the actions of its institutions.

Q2.4: The AVMS Directive today does not impose any independence or other requirements for media regulators – in stark contrast with what is the case in e.g. the telecommunications or energy sector, or for data protection authorities. Would you consider the introduction of such independence requirements for media regulators at EU level a step forward? Would it facilitate the creation of a single market for audio-visual media services? Are there any national legal obstacles to such independence requirements for media regulators? Have there been any problems of undue political or commercial pressure on media regulators in your country?

Independence of regulators is not only essential to make sure that media actors comply with the rules. It is also fundamental to the protection of the integrity and independence of the media landscape in the European Union. Independence plays a fundamental role in guaranteeing freedom of information. Independence also provides the essential wall between politics and independent media and is hence one of the cornerstones of democracy. Moreover, independency requirements for a media regulator strengthens its position, which enables it to facilitate the implementation process of EU-legislation and therefore catalyse the creation of a single market in this field.

Under Dutch law, the members of the board of the Dutch Media Authority, an autonomous administrative body, are appointed (and under strict criteria also dismissed) by the Minister of Education, Culture and Science.[82] Board members are not allowed to be politically active or to be involved in public administration, nor in the media. Despite the fact that the Minister has the formal power to overrule decisions of the Dutch Media Authority in exceptional cases,[83] this system has never resulted in any problems of undue pressure on media regulators and we consider the *de facto* independence of the Dutch Media Authority to be very high.

[82] Art. 12 paragraph 1 Kaderwet Zelfstandige Bestuursorganen. In practice, the other board members are consulted in the selection process of a new member. This has, however, no formal basis in the law.
[83] Art. 7.9 Mediawet 2008.

Q2.5: What have been the most contentious issues in your country in relation to the application of broadcasting laws? (e.g. rules on commercial communications such as product placement or sponsoring? Unsuitable content for minors on television? The dissemination of hate speech? The role of public service broadcasters? Growing media concentration?) Do you think that some areas need further harmonisation through the AVMS Directive?

One of the main objectives of the new AVMS Directive is to ensure a level playing field, in this internet age and given the many new ways of accessing media content. Within the context of the current AVMS Directive, the harmonisation of schemes of self- and (especially) co-regulation have proven to be successful, as can be demonstrated by the effective protection of minors against harmful content. However, one should keep in mind that (regulation of) the media is closely related to a nation's culture. For example, this can bee seen with the classification of content as seriously harmful. Since there is a crucial cultural dimension in the classification of content as harmful or seriously harmful, harmonisation initiatives should leave sufficient space to take cultural differences into account.[84]

The Dutch Media Authority identifies topics of special interest every year in the so-called 'Toezichtbrief' (Regulation Letter) or 'Handhavingsbrief' (Enforcement Letter). In the last three years, these topics have included independence and transparency (2015), protection of viewers, and anticipating on developing technologies (2016), compliance with broadcasting laws in the online domain (while stimulating self-regulation for the areas in which the media authority does not yet have jurisdiction) and governance and internal control in broadcasting organisations (2017).

Discussion on the levels of harmonisation has further arisen with regard to practical questions, such as must-carry obligations, the qualification of content as seriously harmful, editorial responsibility and public-private partnerships.

Q2.6: Have there been any initiatives in your country towards the offering of targeted (or addressable) advertising on television or of personalised content? If so, how was this dealt with under broadcasting/data protection laws? Was there any cooperation between the media regulator and the data protection authority? Do you see a need for an EU-wide harmonised approach?

These developments are highly dependent upon the technological possibilities. Analog television only offered the possibility of one-way traffic. Viewer data was therefore not available for broadcasters. This was also the case at the start of digital television in the

[84] Madeleine de Cock Buning, 'Private Regulation and Enforcement in the EU: Finding the right balance from a Citizen's perspective', in: M.de Cock Buning, L.Senden (ed.), Private Actors in Regulation (working title), to be published by Hart Publishers 2018.

Netherlands. In 2011 UPC (a TV-provider) introduced the Horizon-box platform. This set-top-box made it possible to send data back to the broadcaster, which resulted in, for example, the possibility to recommend videos to specific viewers in the on-demand domains of TV-providers. The possibilities to broadcast personalised commercials are being investigated but this has not resulted in any practical initiatives. In its 2016-'Toezichtbrief', the Dutch Media Authority mentioned the increasing fragmentation of the media landscape. As a next step in this trend, the media authority identified 'personalisation' of media offers under the lead of international companies such as Microsoft, Apple, Google, Facebook and Amazon.[85]

In 2016, the Dutch Data Protection Authority (DPA) investigated KPN and Xs4All, both providers of interactive digital television and found that KPN and XS4ALL created TV-ratings for the purpose of market research without the prior consent of their customers, in circumstances where the ratings could still be linked to identifiable customers. The DPA concluded that XS4ALL and KPN did not provide adequate information to their interactive TV customers about how they collect and process personal data about their TV-viewing behaviour and that this data can be linked to a person's behaviour and interests, which would make it interesting for advertising companies to access this data.[86] The two companies have since then redrafted their privacy statements and data is now processed only for technical purposes.

As television contains an important cross-border element, we consider harmonisation as a desirable next step in the effective protection of citizens against privacy infringements. Therefore, we are in favour of the further harmonisation of the processing of personal data through the new General Data Protection Regulation. The new General Data Protection Regulation will bring further harmonisation to the processing of personal data.[87]

Q2.7: Is the specific regime for copyright licensing for TV and radio broadcasting by satellite and cable (pursuant to Directive 93/83/EEC) still relevant in your country? Have similar rules been applied to online transmissions of broadcasting organisations?

This regime is still applicable and is implemented in the Dutch Copyright Act ('Auteurswet') and the Related Rights Act ('Wet op de Naburige Rechten'). The Dutch Copyright Act was amended by the Copyright Contract Act (which entered into force 1 July 2015) with the view to giving the individual authors and performing artists a stronger position in negotiating

[85] CvdM, 'Toezichtbrief 2016', 22 December 2015, para. 34. < https://www.cvdm.nl/wp-content/uploads/2013/07/Toezichtbrief-2016-Commissariaat-voor-de-Media.pdf
[86] Conclusions Dutch Data Protection Authority [Autoriteit Persoonsgegevens] of the investigation into KPN and XS4ALL digital interactive TV 20 June 2016, Datahttps://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/conclusions_report_xs4all_kpn.pdf
[87] The General **Data Protection Regulation** (GDPR) (**Regulation** (EU) 2016/679)

contracts on copyright transfers with publishers and producers. New technologies and ways of broadcasting content (incl. new platforms) provided authors and performers with additional means of distributing their works, while it became increasingly difficult to negotiate and object against standard provisions in copyright exploitation contracts. The new Copyright Act now contains eight new, non-waivable provisions on exploitation contracts. The main provision is Article 25c which provides a right to 'equitable remuneration'. This remuneration may be reviewed if the exploitation of a work is done in a way that was unforeseen at the time of the initial contract (Article 25c paragraph 6). Additional remuneration may be claimed under the 'bestseller clause', in cases of unexpected success, in Article 25d.[88] The non-use clause Article 25e allows authors to terminate a contract when, after initial acts of exploitation, the copyright holder fails to sufficiently exploit the copyright. In a recent case brought to Court by members of the popular Dutch Band *Golden Earring*, the Dutch Supreme Court (Hoge Raad) found that a copyright contract transferring copyrights can be terminated under Article 25e, but only with a sufficiently serious ground. The court then referred the case to the Court of Appeal for review.[89]

Q2.8: What are the main barriers in your country to cross-border portability of digital content? Do you consider that the country of residence of the consumer should be controlled by the service provider on a regular basis? If yes, how to conciliate such requirement with the data minimisation principle under the GDPR?

In the Netherlands, cross-border portability of digital content may be a problem because of the territoriality of copyright licenses and the business models of online content service providers. The new Regulation (EU) 2017/1128, which will enter into force after twelve months of publication, will change this.[90] Under the new Regulation, subscribers to portable online content services, which are lawfully provided in their Member State of residence, can access and use those services when temporarily present in a Member State other than their Member State of residence. Consideration 30 of the Regulation states that the Regulation should be interpreted in accordance with Article 7 and 8 of Charter of Fundamental rights and — together with the limited list of means of verification in Article 5 of the Regulation— the means of verification should be read in accordance with the minimisation principle under the GDPR. It is yet to be seen how this will be interpreted when the Regulation enters into force.

---

[88] P. B. Hugenholtz, Towards Author's Paradise: The new Dutch Act on Authors' Contracts ,in: Liber Amicorum Jan Rosén, G. Karnell, A. Kur, P-J. Nordell, J. Axhamn, S. Carlsson (ed.), eddy.se ab, Visby 2016, p. 397- 407., K. van den Heuvel, 'What does the new Dutch Copyright Contract Law have to offer?', *Kluwer Copyright Blog* 01-2016 < http://kluwercopyrightblog.com/2016/01/13/what-does-the-new-dutch-copyright-contract-law-have-to-offer/>

[89] HR 7 juli 2017, ECLI:NL:HR:2017:1270 (*Nanada c.s. v. Kooymans c.s.*),.

[90] of the European Parliament and of the Council of 14 June 2017 on cross-border portability of online content services in the internal marketText with EEA relevance,published OJ L 168, 30 June 2017.

3. Digital infrastructures

(Abe IJland & Hans Vedder)

Q3.1: Did your country have rules on net neutrality in place before the adoption of Regulation (EU) 2015/2120? If so, were they more or less strict in comparison to the Regulation? What is the national approach towards practices of zero-rating (which are not explicitly prohibited by the Regulation)?

In answer to the first question, the Netherlands has had rules on net neutrality since 1 January 2013, when the Act of 10 May 2012 amending the telecommunications Act (hereafter: "Tw") entered into force.[91] The rules on net neutrality are now contained in Article 7.4a Tw.[92]

As regards the second and third questions, an integrated answer is provided on the basis of the recent judgment by the Rotterdam District Court in *T-Mobile*. In that case, the court found that there is a discrepancy between Regulation (EU) 2015/2120 and Article 7.4a Tw.[93] Article 7.4 Tw explicitly prohibits zero-rating in a third paragraph that reads as follows:[94]

> "Providers of internet access services shall not make the charges for access services dependent on the services and applications that are offered or used through these access services"

This categorical ban on zero-rating (hereafter: the ban) was discussed during the parliamentary debates leading to the adoption of the Act of 12 October 2016.[95] Initially, the Netherlands tried to uphold the ban by unsuccessfully voting against the Regulation. The Minister later argued that a closer reading of the Regulation allowed the ban to be upheld.[96] On the basis of this ban, the Netherlands Authority for Consumers and Markets (hereafter ACM), the designated NRA pursuant to the Regulation, took action against the telecommunications provider T-Mobile for offering zero-rating for certain music streaming services.[97]

---

[91] The act was published in Stb. 2012, 235.
[92] Following the entry into force of the Act of 12 October 2016 applying the Regulation on net neutrality, Stb. 2016, 409, Article 7.4a has been amended as will be explained below.
[93] ECLI:NL:RBROT:2017:2940. Available at rechtspraak.nl.
[94] Authors translation of 'Aanbieders van internettoegangsdiensten stellen de hoogte van tarieven voor internettoegangsdiensten niet afhankelijk van de diensten of toepassingen die via deze diensten worden aangeboden of gebruikt'.
[95] See fn. 2 above. All parliamentary documents are available at https://zoek.officielebekendmakingen.nl/behandelddossier/34379
[96] This is set out in the Nota naar aanleiding van het verslag. TK 2015-2016 34 379, nr. 6, p. 1, available at: https://zoek.officielebekendmakingen.nl/kst-34379-6.html.
[97] T-Mobile calls this datavrije muziek and it applies to 25 streaming services at this moment, https://www.t-mobile.nl/datavrije-muziek#dienst. In addition, it took action against Tele2 when its terms prohibited customers from tethering their phones, see https://www.acm.nl/nl/publicaties/publicatie/17298/Tele2-past-voorwaarden-op-verzoek-van-ACM-aan/

The ACM, in line with the Minister's position, argued that the Regulation allowed a categorical ban on zero-rating, but this argument was rejected by the District Court.[98] In a nutshell, the Court found no support for the ban in the Regulation; helped in that regard by the fact that an earlier proposal for such a ban by the Netherlands government was rejected by the EU legislature in drafting the Regulation. The judgment further finds that the equal treatment rule applied to *traffic*, rather than the end-user; a conclusion the Court based on reading the first subparagraph, in conjunction with the second and third subparagraph, of Article 3(3) of the Regulation. Pricing modalities such as zero-rating fall, in the opinion of the Court, under the heading of Article 3(1), which contains no categorical prohibition of differentiated prices.

This judgment shows how the Regulation pursues the dual objective of ensuring non-discriminatory treatment of traffic and end-user rights. It may be noted that these two objectives are of a different nature. Traffic exists irrespective of the identity or properties of the parties involved, whereas the end-user rights are inherently connected to the identity of a party connected to the internet. This difference can lead to ambiguity, as the *T-Mobile* case shows. From an end-user perspective, zero-rating is unproblematic because the services used do not impinge on the data limits applicable to a consumer. From the perspective of equal treatment of traffic, the answer is less clear, as zero-rating effectively gives preference to the traffic from the streaming music providers that qualify for the zero-rating. In view of the wide-ranging duty of equal treatment, different treatment between end-users could be argued to be contrary to Article 3(3) of the Regulation. From both perspectives, competitive harm and an impediment to consumer rights could arise, but only in the specific situation whereby, *inter alia*, the provider of internet access services enjoys a degree of market power.[99] However, this requires a case-by-case assessment, such as the one suggested in the BEREC guidelines adopted on the basis of Article 5(3) of the Regulation,[100] and thus would be incompatible with a categorical prohibition. The categorical ban in the Netherlands therefore qualifies as a stricter approach, from the perspective of non-discriminatory traffic management, as it arguably results in a lower level of protection from the perspective of the end-user. In view of its incompatibility with the Regulation, the Act is not applied by ACM, which has coincidentally decided not to appeal the judgment in *T-Mobile*.[101]

Q3.2: Should the EU go further in creating a single market for telecommunications networks or services (and introduce e.g. an EU-wide licensing scheme)? Did your national authorities adopt any special broadband measures and where they the result of EU intervention or adopted at own initiative?

---

[98] The core of the reasoning can be found in paragraph 6.5 of the judgment, *supra* fn.934.
[99] In this regard, the analysis continues as an analysis of vertical foreclosure effects.
[100] Such guidelines have been adopted and are available at http://berec.europa.eu/eng/document_register/subject_matter/berec/download/0/6160-berec-guidelines-on-the-implementation-b_0.pdf.
[101] https://www.acm.nl/nl/publicaties/publicatie/17251/ACM-niet-in-hoger-beroep-tegen-uitspraak-over-netneutraliteit/.

With regard to the second question, ACM takes measures with regard to the telecommunications sector on the basis of Chapter 6a.1 Tw. This Chapter stipulates that ACM must analyse relevant telecommunications markets as determined in the Commission recommendation on relevant markets susceptible to ex-ante regulation.[102] In its analysis, ACM must consider whether these markets are competitive and whether any companies operating in them have significant market power. If the latter is true, ACM may impose obligations on companies with considerable market power to provide access — at capped prices — for competitors to a wide range of their facilities, including networks, facilities, wholesale services, technical interfaces and protocols.

For example, after a market analysis study, ACM concluded that the market for unbundled access was not competitive and that KPN had significant market power. Consequently, ACM imposed various access requirements and price caps on KPN for the statutory maximum period of three years (at which time ACM has to reconsider its analysis).[103]

As regards to measures implemented by the central government, the Netherlands is well on track to meeting the goal in the Digital Agenda of universal access to internet with speeds of at least 30 Mbps by 2020.[104] In order to meet the goal of universal access to internet with speeds of at least 100 Mbps by 2025, as formulated in the strategy on Connectivity for a European Gigabit Society, the Minister for Economic Affairs has proposed initiatives for sharing knowledge with local governments about state aid for network capacity expanding projects, and about technical subjects related to the expansion of broadband capacity.[105]

Q3.3: Are there legal issues on spectrum management in your country? If yes, how have they been solved?

In the Netherlands, scarce spectrum is usually allocated by auction.[106] The courts in the Netherlands have generally ruled, following challenges to specific governmental decrees by which spectrum was allocated, that regulations concerning spectrum management were not

[102] Commission Recommendation of 9 October 2014 on relevant product and service markets within the electronic communications sector susceptible to ex ante regulation in accordance with Directive 2002/21/EC of the European Parliament and of the Council on a common regulatory framework for electronic communications networks and services, OJ 2014, L295/79.
[103] ACM decision 17 December 2015, marktanalyse ontbundelde toegang, available at: https://www.acm.nl/nl/publicaties/publicatie/15087/Marktanalysebesluit-ontbundelde-toegang-2016--2019/
[104] According to the legislative proposal for implementation of the Broadband Directive 2014/61/EU, 97% of Dutch households and 91% of companies had access to 30 Mbps internet, see Kamerstukken II, , 2016-2017, 34739 nr. 3, p.1, available at: https://zoek.officielebekendmakingen.nl/kst-34739-3.html
[105] Letter from the minister for Economic Affairs to parliament on fast internet in peripheral areas of 16 December 2016, available at: https://www.rijksoverheid.nl/documenten/kamerstukken/2017/07/03/kamerbrief-over-snel-internet-in-het-buitengebied
[106] For example the Multiband (800, 900 and 1800 Mhz) auction of 2012 and the 2.6 Ghz auction of 2010. A press release for the Multiband auction is available at: https://www.agentschaptelecom.nl/sites/default/files/press-release-dutch-frequency-auction.pdf. The Telecommunications Act 3.10 also allows for allocation by contest, but auctions are preferable according to government policy, see also the Radio Spectrum Memorandum Policy 2016, p. 10, available at: https://www.government.nl/documents/reports/2017/03/07/radio-spectrum-policy-memorandum-2016 , and ECLI:NL:RBROT:2002:AE5810.

in breach of European legislation.[107] However, the government has recently published its third Radio Spectrum Policy Memorandum — setting out medium-to-long term policy goals — and it remains to be seen whether the resulting initiatives will lead to fresh challenges following future auctions.[108]

Q3.4: Have questions linked with the independence of NRA's been raised in your country? If yes, did they lead to legal challenges? How have they been solved?

ACM is the designated NRA for the Dutch telecommunications sector. In the period leading up to the creation of ACM in 2013, one author opined that the institutional structure of the then-future organisation would not satisfy the criteria for independence as laid down in various EU Directives concerning regulated sectors.[109] According to this author, ACM would lack institutional independence from the Ministry of Economic Affairs, *inter alia* because ACM would not possess legal personality, and the ministry would therefore provide its budget and personnel.[110]

Coincidentally, the question of whether ACM should be given distinct legal personality — to have its own personnel and budget — was also raised in this context during the parliamentary debate preceding the creation of ACM.[111] The Minister for Economic Affairs responded that these features where not necessary to satisfy the requirements of independence in the EU Directives. Accordingly, ACM was created as an independent administrative body without its own legal personality, personnel or budget.

With regard to the institutional independence of ACM and its personnel, Dutch law stipulates that personnel that are made available to independent administrative bodies (such as ACM) report exclusively to the independent administrative body concerned.[112] The Act establishing the ACM (*Instellingswet Autoriteit Consument en Markt*) furthermore contains a provision which precludes the Minister from issuing instructions in individual cases to ACM personnel or its board.[113] Therefore, the Minister has no formal involvement e.g. in the market analyses on unbundled access that ACM conducts on a three-yearly basis in the telecommunications sector, as mentioned under Q3.2 above.

---

[107] For example in the Multiband case, ECLI:NL:RBROT:2014:7917, the court ruled that a provision for new entrants in the regulation on the method of auctioning was not in breach of the Authorisation directive 2002/20/EC, the Framework directive 2002/21/EC or state aid law. See also J. Wolswinkel, 'The Allocation of Radio Frequencies in the Netherlands', in: *Scarcity and the State II*, P. Adriaanse et al (eds), Intersentia:2016.
[108] See note 17 above.
[109] Van Eijk, N. (2012). ACM onafhankelijk? Jaarboek - Koninkijke Vereniging voor de Staathuishoudkunde, 2012, 299-230.
[110] With the exception of the regulatory task of ACM with regard to the transport sector, for which the Minister for Infrastructure and Environment is responsible.
[111] Kamerstukken II 2011/12, 33186, 3, p. 6-7, available at: https://zoek.officielebekendmakingen.nl/kst-33186-C.html.
[112] Kaderwet zelfstandige bestuursorganen (stb. 2014, 483), art. 16.
[113] Instellingswet Autoriteit Consument en Markt (stb.2013, 102), art. 9. Also see CBb 29 juni 2010, ECLI:NL:CBB:2010:BM9470, in which the Trade and Industry Appeals Tribunal judged that the minister had issued an instruction concerning an individual case.

With regard to policy, although the Minister for Economic Affairs has the competence to formulate policy for the telecommunication sector, it has been recognized that the Minister must take the requirements of independence for NRA's in the EU Directives into consideration when formulating policy for ACM.[114] As regards to policy formulated by ACM itself, the Minister does not have competence to nullify ACM's policy or legislation with regard to the energy, postal, telecommunications and transport sectors.[115] Although ACM is bound to inform the minister of its intended policy decisions with regard to these sectors, the minister has no right of veto with regard to such decisions.

To the knowledge of the authors, no concerns about ACM's independence have, to date, resulted in legal challenges to ACM's legitimacy as an independent NRA.

4. Data in the digital economy

(4.1 – 4.3: Hielke Hijmans, Emilie van Hasselt)

Q4.1: How is your country preparing for the entry into force of the General Data Protection Regulation in May 2018? Are there any specific legislative proposals or executive measures in preparation?

The preparation in the Netherlands for the application of the General Data Protection Regulation (GDPR) takes place at various levels, involving public authorities as well as the private sector.

The important changes in the European legislative framework of data protection require an overhaul of the national law for data protection (*Wet bescherming persoonsgegevens*), which will be repealed. The main legislative instrument, enabling full application of the GDPR within the national jurisdictional and administrative frameworks, will be the implementing law of the GDPR (*Uitvoeringswet Algemene verordening gegevensbescherming*, hereafter: "the implementing law").[116] On 9 December 2016, a draft of the implementing law was published by the Dutch Ministry of Security and Justice for public consultation, to which the Ministry received many responses.[117] An important and substantial reaction was given by the Dutch Data Protection Authority (*Autoriteit Persoonsgegevens*, hereafter: "DPA") and was made public on its website.[118]

The GDPR also completely changes the landscape for the national independent supervisory data protection authorities and how they exercise control. Therefore, DPA commissioned a consultancy firm to calculate the consequences of the new regime for data protection in the EU,

[114] Kamerstukken II 2011/12, 33186, 3, p. 11, Kamerstukken II 2010/11, 32814, 3, p. 24.
[115] Instellingswet Autoriteit Consument en Markt (stb.2013, 102), art. 10.
[116] https://www.internetconsultatie.nl/uitvoeringswetavg/details.
[117] https://www.internetconsultatie.nl/uitvoeringswetavg/reacties
[118] https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/advies_uitvoeringswet_avg.pdf.

and for its resources. Sufficient resources are needed to perform its tasks and exercise its powers in accordance with the Articles 57 and 58 GDPR in an independent and effective manner.[119] In its report, the consultants took the view that the new situation is completely different from the former situation. It emphasized the expected growth of the number of complaints, the new requirements for handling complaints, and the significant increase of European cooperation and *ex officio* investigations, which will require more systemic control. It also mentioned the resources which would be needed for new tasks under the GDPR, such as promoting awareness of public and controllers, prior consultation relating to data protection impact assessments, certification and accreditation, and data breaches. It considers that this new reality will require an increase of staff from the current total of 72 to 185-270 staff (depending on the scenario chosen).[120] The national budget for 2018, as presented by the Dutch government in September 2017, provided for an additional annual budget of €7 million, almost doubling the existing budget of DPA.

This contribution further focuses on a few key components of the implementing law.

First, the relationship between the Regulation and national law is addressed in the explanatory memorandum of the proposed implementing law as a layered legislative structure. The Dutch government intends to use its margin of manoeuver in a policy-neutral manner; meaning that, where possible, existing national policies should be affected as little as possible. It also intends to limit the introduction of additional national law and not to use all specifications and derogations in the GDPR. The draft law does, however, contain precise provisions on specific categories of data such as biometric data.

Second, as regards to the the setting up of DPA and the guarantees of its independence, as a consequence of the complete independence of the data protection authorities,[121] a few provisions of the national framework law for regulatory authorities (*Kaderwet zelfstandige bestuursorganen*) will not be applicable to the DPA. The Minister will not be entitled to give policy guidance to the DPA, nor will he or she have the power to annul its decisions. The responsible minister has these powers in relation to all other regulators in the Netherlands.

The Dutch rules on the appointment of the members of the DPA will not be changed. These persons will be appointed by the King, on a proposal by the Minister. Arguably, this procedure does not fulfil the transparency requirements of Art 53 GDPR.

Third, on the embedding of the DPA into the national administrative law system, the general legislation on administrative law (*Algemene wet bestuursrecht*) contains provisions on the tasks

[119] This control is an essential component of the right to data protection, Case C-362/14, Schrems, EU:C:2015:650, at 41.

[120] https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/brief_a_dhr_dijkhoff_inzake_aef.pdf .

[121] Further read: Hielke Hijmans, The European Union as Guardian of Internet Privacy, Springer 2016, Ch. 7.

and powers of authorities that need to be reconciled with the long catalogue of tasks and powers in the GDPR.

Fourth, the draft implementing law provides that it applies to the processing of personal data in the context of activities of organisations in the Netherlands. This means that the criterion for applicability is the establishment of an organisation, not whether the fundamental rights of individuals in the Netherlands are affected; for instance, when services are offered on the internet from another Member State. By comparison, the German implementing law[122] takes the opposite view.

The DPA has provided a long and specific advice on the draft implementing law. Some interesting elements are:

- The DPA should have legal personality.
- The Dutch government should refrain from explaining the uniformly-applicable GDPR, apart from explanations which are not obvious.
- The implementing law should not exceed the discretionary powers provided by the GDPR, particularly in relation to biometric and genetic data.
- The implementing law should include rules on the personal data of deceased persons.[123]

Q4.2: How are businesses in your country adapting to the new requirements of the GDPR such as those related to consent, impact assessments, privacy by design and by default?

Businesses (and public bodies) seem increasingly aware of the need to review and adapt their internal processes to comply with the new requirements of the GDPR. Consultancy firms are also now offering a range of IT tools and compliance checklists. One of the challenges for businesses in the Netherlands, however, in preparing for the GDPR, is that the implementing law has not yet been submitted to Parliament (see above under Q4.1). Moreover, other than the advice given by the DPA in relation to the draft law (see above under Q4.1), the available guidance given by the DPA has been limited to a few documents published on its website. An important document was issued on 13 April 2017 and outlines ten steps to help businesses prepare for the GDPR.[124] The authority also gave guidance on various other issues, such as children's on-line data and on policies to be adopted by schools.

Q4.3: 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

[122] https://www.datenschutz-notizen.de/das-deutsche-datenschutzgesetz-wurde-angepasst-die-eu-datenschutz-grundverordnung-kann-kommen-5018053/.
[123] In accordance with Recital 27 of the GDPR.
[124] https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/in_10_stappen_voorbereid_op_de_avg.pdf

specific legislative measures or regulatory opinions/decisions in this area? What is the status of the policy debate?

Big Data is perceived as one of the key issues from a legal point of view. To ensure the proper use of Big Data, along with safeguards for privacy and other fundamental rights, the government requested the Netherlands' Scientific Council for Governent Policy (*Wetenschappelijke Raad voor Regeringsbeleid,* hereafter: "WRR") to advise on the topic 'Big data, privacy and security.' The government's request of 26 May 2014 focused on four key issues:

- Is it possible to draw a clear distinction in privacy and data protection law between access to data, collection of data, and use of data? And if that is possible, should such a distinction in fact be made?
- How can the process of profiling, and data mining, and other techniques of data-analysis be made sufficiently transparent with a view to security without damaging their effectiveness for security policy?
- What does the development of quantum computers mean for the process of data processing and protection (encryption)?
- What is the impact of Big Data on government data management systems, and how can citizens be involved and influence this process?

On 31 January 2017, the WRR published a policy brief entitled 'Big Data and Security Policies: Serving Security, Protecting Freedom".[125] In this document, which is based on the WRR Report 'Big Data in a Free and Secure Society' (*Big Data in een vrije en veilige samenleving*)[126], the WRR argued that the use of Big Data in the field of security requires a new regulatory framework. The WRR stated in particular that the emphasis in that framework should be on regulating data analysis and use, rather than on intensifying the regulation of data collection. According to the WRR, it is in data analysis and use that the biggest opportunities and risks of Big Data lie and where new rules are required.

As regards to IoT, the Rathenau Instituut, a Dutch research institution specialized in technology and society, issued a report which highlights that IoT will create new opportunities in the sharing economy.[127] For example, the risk of misuse of goods, theft or illegitimate use will diminish when machines can communicate. This report contains a number of specific recommendations, *inter alia*, that the government should clarify the legal status of sharing platforms, that the government could appoint trusted third parties to supervise platforms and that arrangements could be made to ensure that users can have their data ported to other platforms.

[125] https://english.wrr.nl/topics/big-data-privacy-and-security/news/2017/01/31/wrr-policy-brief-on-use-of-big-data-in-the-security-domain
[126] https://www.wrr.nl/publicaties/rapporten/2016/04/28/big-data-in-een-vrije-en-veilige-samenleving
[127] Report published on 30 May 2017, available via https://www.rathenau.nl/nl/publicatie/eerlijk-delen-waarborgen-van-publieke-belangen-de-deeleconomie-en-de-kluseconomie

Concerning Machine-to-machine generated data, the Authority for Consumers and Markets ("ACM") announced in a press release dated 13 October 2015[128] that it wanted to tighten the monitoring of 097-numbers in light of the mandatory use of this category for mobile data communication such as M-2-M and IoT. ACM found that most mobile communications providers did not provide sufficient information to consumers and business about this number range and highlighted that laptops were still sold with a data-only connection and 06-number, instead of the mandatory 097-numbers. In a press release of 19 June 2017, ACM announced that the pressure on mobile numbers continues to be strong because of new applications.[129]

Recently, members of the Dutch House of Representatives expressed their concern that IoT developments have led to an increased number of poorly protected devices. In light of the risk of cyber-attacks, they requested that the government investigate whether minimum safety requirements could be imposed and enforced to protect consumers.[130] Subsequently, in Dutch media, the possibility of an 'Internet of Things quality label' was raised.[131]

Concerning automated cars, the government approved the Autonomous Vehicles (Trials) Bill on 24 February 2017, which allows trials for autonomous cars without a driver on board.[132] By removing legal barriers, Infrastructure Minister Melanie Schultz aims to give manufacturers more opportunities to test autonomous vehicles. Under the new bill, the Road Transport Agency (RDW) will decide in advance, in cooperation with the Institute for Road Safety Research (SWOV), the road authority and the police, on permits to test vehicles that are controlled remotely by human operators on public roads. Permits may, for example, stipulate that the manufacturer must implement measures to make other road users aware that the vehicle is remotely controlled. Based on the road tests, the government will decide on whether further regulation is necessary.

Policy debate regarding smart city proposals are ongoing. There are a number of cooperation initiatives between municipalities that aim to define a common strategy.[133] In this context, one of the contentious issues is the use of Wifi-tracking technology in public-private partnerships. In this respect, it can be noted that the DPA imposed an order subject to penalty payments on a company that offered Wifi-tracking in and around shops.[134] In an official investigation, the DPA found that the collection of personal data by means of Wifi-tracking can be necessary for legitimate business interest. However, in this particular case, the DPA found that the necessary

[128] https://www.telecompaper.com/news/acm-wants-better-monitoring-of-097-numbers--1107446
[129] https://www.acm.nl/en/publications/publication/17355/Pressure-on-mobile-phone-codes-continues-to-be-strong-because-of-new-applications/

[130] MotieHijink and Verhoeven, TK 2016-2017, 26 643, nr. 467.
[131] https://www.nrc.nl/nieuws/2016/11/20/d66-wil-keurmerk-voor-beveiliging-iot-apparaten-a1532668
[132] https://www.government.nl/latest/news/2017/02/24/driverless-cars-on-the-roads
[133] http://gsc3.city/files/strategie/NL_Smart_City_Strategie_Executive_Summary.pdf
[134] https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-legt-wifi-tracker-bluetrace-last-onder-dwangsom-op

guarantees — to protect the interests of data subjects outside the premises of retailers — were not in place. The authority requested, in particular, that adequate information be provided to the public about the fact that they are being registered by way of Wifi-tracking, and being tracked unnoticed via their mobile device.

The DPA also intervened in a project by the municipality of Arnhem and requested that the collection of individual data by means of 'trash disposal cards' (*afvalpas*) be terminated because of its findings that the collection of personal data in this manner is not currently necessary for exercising public tasks.[135] In a press release dated 2 May 2017 regarding this matter, the DPA highlighted the importance of clarifying the purpose of data collection (in, e.g. tax collection), the importance of informing residents about this purpose and about the use of their data (which must be proportionate) and the need to adequately protect the 'trash disposal cards'.

(4.4: Stefan Kulk, Remy Chavannes)

Q4.4: Since the CJEU's controversial judgment in May 2014 in the Google Spain (or Costeja) case, the so-called "right to be forgotten" (or to be delisted) has received a lot of attention in Europe and beyond. What is the legal status in your country? Are complaints being brought before the data protection authority and/or courts? Has there been a growing body of case law in this regard? How is the balance struck between the individual's right to data protection and the other interests at stake (in particular the search engine's commercial freedom, the public's right to information and the author's right to free expression)?

Since the CJEU's decision in the *Google Spain* case, the right to be delisted has been the topic of quite a number of Dutch court cases.[136] The CJEU in *Google Spain* considered in particular the individual's right to data protection and privacy, the public's right to information, and the search engine operator's economic interests.[137] With regard to the search engine's role, the CJEU focused primarily on the processing and dissemination of personal data by the search engine, and its impact on the individual's right to privacy. In contrast, the Dutch courts in a number of

[135] https://www.autoriteitpersoonsgegevens.nl/nl/nieuws/ap-gemeente-arnhem-past-afvalsysteem-aan

[136] For an overview of early case law, see: S. Kulk and F.J. Zuiderveen Borgesius, 'Freedom of expression and 'right to be forgotten' cases in the Netherlands after Google Spain', *European Data Protection Law Review* 2015-2, p. 113-125. See also the summary of recent cases included in the Dutch DPA's reports on mediation requests in delisting cases, most recently: *Autoriteit Persoonsgegevens 11 May 2017,* https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/overzicht_bemiddeling_ap_bij_verwijdering_resultaten_zoekmachines_mei_2017.pdf

[137] CJEU 13 May 2014, C-131/12, ECLI:EU:C:2014:317 (Google Spain, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González).

cases also considered the search engine's operator right to freedom of information, the important role of search engines in facilitating access to online information, and the need for courts to exercise restraint in imposing restrictions on their activities so as to protect their catalogue function.[138]

One delisting claim has so far made it to the Dutch Supreme Court, filed by a man convicted of attempting to procure the contract-killing of a competing escort boss. In its decision of 24 February 2017, the Supreme Court held that, in delisting cases related to search engines, it follows from the *Google Spain* decision that the right to privacy, as a rule, overrides the interests of the search engine and the interest of internet users searching for information.[139] However, it also restated the rule from *Google Spain* that a data subject only has a right to delisting if the conditions of (the Dutch implementation of) Articles 12(b) and 14(a)(1) of the Privacy Directive are in fact satisfied. As a consequence, there remains a measure of uncertainty about the applicable norm, and the extent to which (and manner in which) the various competing fundamental rights are to be considered in delisting cases.[140]

The DPA has acted as a mediator in several cases in which the search engine operator – usually Google – denied a removal request. In 2016 and again in 2017, the DPA published a report on its decisions in these mediation cases; helpfully including brief summaries of the published court decisions in delisting cases.[141] As of May 2017, the DPA had received mediation requests from 155 individuals. This represents about 1% of the people whose removal requests have been denied by a search engine.[142]

In 70 cases, the DPA decided not to mediate — either because the search engine did not clearly violate Dutch data protection law, the facts of the case were unclear, or there were ongoing legal proceedings. In 54 cases, the DPA did attempt to mediate; in 37 of those cases, search results were eventually removed. In 14 cases, Google stood by its decision not to remove the search results.

---

[138] Rb. Amsterdam 24 September 2014, ECLI:NL:RBAMS:2014:6118; Rb. Amsterdam 12 February 2015, ECLI:NL:RBAMS:2015:716; Rb. Amsterdam 24 December 2015, ECLI:NL:RBAMS:2015:9515; Rb. Den Haag 12 January 2017, ECLI:NL:RBDHA:2017:264.
[139] HR 24 February 2017, ECLI:NL:HR:2017:316.
[140] HR 24 February 2017, ECLI:NL:HR:2017:316, par. 3.5.6.
[141] *Autoriteit Persoonsgegevens*, 25 May 2016; https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/overzicht_bemiddeling_autoriteit_persoonsgegevens_bij_verwijdering_zoekresultaten_google_0.pdf; and *Autoriteit Persoonsgegevens*, 11 May 2017, https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-bemiddelt-52-keer-bij-verwijdering-zoekresultaten-google-en-bing . For an English summary of the most recent report, see https://www.stefankulk.nl/index.php/1770/dutch-dpa-releases-new-data-about-the-right-to-be-forgotten/.
[142] As of 5 July 2017, Google has received just under 33,000 removal requests, regarding more than 117,000 URLs, of which 53,6% was not removed. See: https://www.google.com/transparencyreport/removals/europeprivacy/?hl=en. The statistics for Microsoft's Bing search engine show a rejection rate of 52% for the Netherlands: https://www.microsoft.com/en-us/about/corporate-responsibility/crrr.

It is not clear how the right to be delisted relates to the in principle prohibition to process sensitive data and data relating to criminal convictions and offences. *Google Spain* established that a search engine operator processes personal data by indexing, ranking and displaying it on search engine result pages.[143] If such data is sensitive, would the search engine operator then, in principle, be prohibited from processing such data? Lower Dutch courts have given conflicting rulings with respect to the way in which a search engine operator processes sensitive data. In one case, the Hague District court considered the search results (including snippets) rather than the source pages, and determined that these did not contain facts indicative of criminal conduct. On that basis, it concluded that Google had not processed any criminal personal data regarding the data subject.[144] Google, in essence, is not responsible for the processing of data on the pages it links to. The Midden-Nederland District court did not make the same distinction between search results and source pages, but similarly held that the prohibition on processing criminal personal data did not apply because the source publications at issue only contained *allegations* of criminal misconduct, which had not been investigated by the authorities and which the data subject denied.[145] The Overijssel District Court explicitly held that the contents of the linked-to page should also be part of the analysis and concluded that a search result pointing to a Facebook post about the data subject's court appearance for child sex abuse involved the processing of sensitive personal data that was *per se* prohibited. It also held that a thumbnail of a business photo of the man was sensitive personal data because it revealed his race, but rejected the delisting request on the grounds that he had authorized the photo to be published.[146]

In a recent ruling regarding a delisting request, related to a lawyer's conviction for a knife crime, the Court of Appeals of the Hague held that a search engine operator can potentially rely on the journalistic exemption, and that there is still room to consider the right to freedom of expression if search engine operators process sensitive data. The Court considered par. 85 of *Costeja,* in which the CJEU referred in passing to the journalistic exemption. The Court concluded that in some cases (as the pointed out by the CJEU), the source publication might be able to invoke the journalistic exemption in circumstances where the search engine can not; and that the CJEU could not have intended to categorically exclude the possibility of taking into account freedom of expression in delisting cases relating to special categories of personal data.[147] In considering the freedom of expression, factors — such as the role that the individual plays in public life — may justify sensitive data being processed by the search engine operator, regardless of the prohibition against processing sensitive data.

[143] CJEU 13 May 2014, C-131/12, ECLI:EU:C:2014:317, par. 28 (Google Spain, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González).
[144] Rb. Den Haag 12 January 2017, ECLI:NL:RBDHA:2017:264.
[145] Rb. Midden-Nederland 20 February 2017, ECLI:NL:RBMNE:2017:805.
[146] Rb. Overijssel 24 January 2017, ECLI:NL:RBOVE:2017:278, par. 4.16.
[147] Hof Den Haag 23 May 2017, ECLI:NL:GHDHA:2017:1360, par. 5.8 - 5.11.

In the handful of cases where Google has been ordered to delist search results, the order has been restricted to Google Inc.; claims against the local entity, Google Netherlands, have been rejected on the grounds that it is not the data controller and not capable of carrying out a delisting order. There has been some discussion about the extent of a delisting order against Google Inc., in particular the question of whether delisting should be carried out globally. In general, Dutch courts have focused on search results where Google Search is accessed from the Netherlands, or EU versions of Google Search.