Stanford – Vienna
Transatlantic Technology Law Forum

A joint initiative of
Stanford Law School and the University of Vienna School of Law

Transatlantic Antitrust and IPR Developments

Bimonthly Newsletter

Issue No. 2/2021 (October 18, 2021)

Contributors:

Dayana Zasheva, Gabriel M. Lentner, Marie-Andrée Weiss, Mauritz Kop, Sebastian Pech

Editor-in-chief: Juha Vesala

Contents

About the contributors

Gabriel M. Lentner is an Assistant Professor of Law at the Danube University Krems and currently a Visiting Scholar at Harvard Law School. He holds a Ph.D. in International Law, a diploma with the highest distinction in European Studies from the University of Vienna (2010), and a diploma in Law & Logic from Harvard Law School and the European University Institute in Florence (2013). His main research interests are international investment law, EU law, and public international law. As a TTLF Fellow, his current research focuses on the protection of intellectual property rights through international investment agreements. Dayana Zasheva is a Research and Teaching Assistant at Danube University Krems.

Marie-Andrée Weiss is an attorney admitted in New York and in Strasbourg, France. Before becoming an attorney, she worked for several years in the fashion and cosmetics industry in New York as a buyer and a director of sales and marketing. She graduated from the University of Strasbourg in France with an M.A. in Art History, a J.D. in Business Law, an LL.M. in Criminal Law, and an LL.M. in Multimedia Law. Marie-Andrée also graduated from the Benjamin N. Cardozo School of Law in New York City with an LL.M. in Intellectual Property Law. She is an attorney in New York and her solo practice focuses on intellectual property, privacy, data protection, and social media law. As a TTLF Fellow, Marie-Andrée's current field of research is a comparison of the powers given to users by the EU Digital Service Act and by the Facebook Oversight Board.

Mauritz Kop is a Stanford Law School TTLF Fellow, Founder of MusicaJuridica and strategic intellectual property lawyer at AIRecht, a leading 4th Industrial Revolution technology consultancy firm based in Amsterdam. His work on regulating AI, machine learning training data and quantum technology has been published by Stanford, Harvard,Yale and Berkeley scholarly journals. Mauritz delivered copyright expertise to the European Parliament during the EU Copyright Directive legislative process. He held IP, music and technology law guest teaching positions at Leiden University, Maastricht University and Utrecht University and provided postdoc legal training to Supreme Court judges, lawyers and legal professionals at Radboud University. Mauritz is a member of the European AI Alliance (European Commission), the Dutch Copyright Society (VvA), CLAIRE (Confederation of Laboratories for Artificial Intelligence Research in Europe), the ECP|Platform for the Information Society, and the World Economic Forum (WEF). He is author of numerous articles and blogs about legal and ethical aspects of exponential innovation in industrial sectors such as health-care, agrifood, and entertainment & art, and is a frequently asked international conference speaker on topics in the nexus of AI and Law. His present cross-disciplinary, comparative research focuses on human-centered AI, quantum-ELSPI and sustainable disruptive innovation policy pluralism.

Sebastian Pech is a lawyer and scholar from Germany. He graduated in law from Ludwig Maximilian University of Munich, Germany, earned an LL.M. in IP/IT law at the Duke University School of Law, and a Dr. jur. (Ph.D. in law) at the University of Bayreuth, Germany. His experience includes, among others, positions at the legal publishing house C.H.Beck, the Institute for Copyright and Media Law (IUM), and law firms specialized in IP and IT law. Sebastian's research focuses on the effects of digital transformation on the legal system, especially the challenges (and opportunities) for technology, copyright, and media law, from both the European and the US perspective. He also publishes regularly on these topics. He is a member of the German-American Lawyers' Association (DAJV), the German Association for the Protection of Intellectual Property (GRUR), and the Copyright Society of the USA (CSUSA). Sebastian has been a TTLF Fellow since 2021.

Intellectual Property
United States

Embedding: Infringing in the Second Circuit but Not in the Ninth Circuit Under Server Test

By Marie-Andrée Weiss

United States District Judge Jed Rakoff, from the Southern District of New York (SDNY), published an opinion on 30 July 2021, which has generated a lot of attention, as it rejected the so-called server test in an embedding case. Caselaw is constantly changing in this area and may lead to a circuit split, as courts in the Second Circuit and courts in the Ninth circuit interpret differently whether embedding a work is displaying it under the Copyright Act.

The case is *Nicklen v. Sinclair Broadcasting Group, Inc., et al*, (S.D.N.Y. 30 July 2021).

Does embedding infringe plaintiff's exclusive display right?

Nicklen argued that Defendant, by embedding his original post into an article published online, had displayed the protected work, in breach of the Copyright Act which provides owners of copyright the exclusive right to display the protected work.

17 U.S.C. § 106(5) provides that copyright owners have the exclusive right to publicly display literary, musical, dramatic, and choreographic works, pantomimes, pictorial, graphic, or sculptural works, but does not mention videos or films. However, 17. U.S.C. §101 defines "display" as showing a copy of a work "*either directly or by means of a film, slide, television image, or any other device or process or, in the case of a motion picture or other audiovisual work, to show individual images nonsequentially*." The Copyright Act defines "copies" as "*material objects, other than phonorecords, in which a work is fixed by any method now known or later developed, and from which the work can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device*."

The Ninth Circuit "server test"

Defendant invoked the Ninth Circuit's "server rule" in defense. The Ninth Circuit Court of Appeals approved a lower court in Perfect 10, Inc. v. Amazon.com, Inc. which had found that the owner of a computer not storing an electronic information is not displaying that information. If the images remain on a third party's server, they have not been fixed in the memory of defendants' computers, and therefore are not infringing. An image is displayed under the Perfect 10 server test only if a website publisher "*us*[*es*] *a computer to fill a computer screen with a copy of the photographic imaged fixed in the computer's memory*." This definition can be

applied to embedding, as an image embedded using the API is fixed on the server of the site where it was published by the copyright owner, Instagram's servers, in our case.

The Goldman v. Breitbart and the Sinclair v. Ziff Davis cases

Indeed, Judge Rakoff found, in our case, that, by embedding the video, Defendant had displayed the video withing the meaning of the Copyright Act, noting that the display right is "*technology-neutral*." The embed code allows the video to be displayed and thus "*embedding… falls squarely within the display right*." He quoted the 2018 S.D.N.Y. *Goldman v. Breitbart* case (for some background on this case, see TTLF Newsletter post here) and found it to be "*a poor fit for this case*."

In *Goldman*, plaintiff had taken a photograph of football player Tom Brady walking on an East Hampton street with basketball player Kevin Durant. The photo became viral on social media and was embedded on defendant's site to illustrate an article pondering whether Brady was actively helping the Boston Celtics basketball team recruit Durant. Defendant had evoked the "server test" in defense, but United States District Judge Katherine B. Forrest held the test only applied to cases where the defendant is a search engine, and that "*outside of the Ninth Circuit, however, the Server Test has not been widely adopted*..."

In another embedding S.D.N.Y. case, Sinclair v. Ziff Davis, LLC., United States District Judge Kimba M. Wood dismissed plaintiff Stephanie Sinclair's claim for copyright infringement against Mashable, Inc. and its parent company, Ziff Davis, which alleged that defendants had infringed her copyright when Mashable posted one of her photograph on its website. Judge Wood had found that Mashable had used Sinclair's photograph pursuant to a valid sublicense from Instagram.

In *Nicklen*, Judge Rakoff did not discuss the issue of whether a sublicense had been granted but critiqued the server rule as forcing photographers promoting their work on Instagram to "*surrender*[ ] *control over how, when, and by whom their work is subsequently shown -- reducing the display right, effectively, to the limited right of first publication that the Copyright Act of 1976 rejects*."

Defendants' argument that Nicklen only had to remove his video from Instagram to remove it from Sinclair's website as well did not pass muster with Judge Rakoff, as "*the Copyright Act* [*does not grant*] *authors an exclusive right to display their work publicly only if that public is not online*." For Judge Rakoff, "[*t*]*he server rule is contrary to the text and legislative history of the Copyright Act*," which defines "display" as showing a copy of the work, not "*to make and then show a copy of the copyrighted work*."

As Judge Rakoff found that Defendant's fair use affirmative defense could not be resolved at the motion to dismiss stage, he denied its motion to dismiss.

Towards a circuit split?

A few days after the *Nicklen v. Sinclair case*, United States District Judge Charles R. Breyer from the Northern District Court of California granted Instagram's motion to dismiss in a class action case, Hunley v. Instagram LLC., where two photographers, representative of the class, had sued Instagram, claiming that the company was secondarily liable for copyright infringement for allowing third parties to use its embedding tool to display photos and videos posted on Instagram. The complaint alleged that Instagram's "embedding" tool was used "*to generate substantial revenue for its parent, Facebook, Inc., by encouraging, inducing, and facilitating third parties to commit widespread copyright infringement*."

Judge Breyer stated that, "[*u*]*nder Perfect 10, the third parties do not violate Instagram users' exclusive display*. … *Because they do not store the images and videos, they do not "fix" the copyrighted work in any "tangible medium of expression." … Therefore, when they embed the images and videos, they do not display "copies" of the copyrighted work*."

This case is unusual as "[*t*]*he parties agree that Instagram is not a direct copyright infringer*" and it is not the defendant, but the plaintiff, who invoked the S.D.N.Y. *Nicklen* case, arguing that *Perfect 10* should be "*cabined*" to search engine cases, or cases when users must click a hyperlink to view an image, and that the server test should not apply to cases where an image shared on social media is embedded on a third-party website.

Regardless, Judge Breyer put this argument firmly to rest, as :

"*unlike the [S.D.N.Y.] this Court is not free to ignore Ninth Circuit precedent. And in purporting to establish a test for when a computer displays a copyrighted image, Perfect 10 did not state or indicate that its holding was limited to the unique facts presented there. Thus, this Court must faithfully apply Perfect 10 absent a contrary Ninth Circuit or Supreme Court ruling*."

As the Second Circuit sees embedding as infringing while the Ninth Circuit does not, it will be interesting to see if (when?) the Supreme Court will accept to review a case about embedding which would allow the Court to weigh in on the server test.

Other Developments

European Union

EU Artificial Intelligence Act: The European Approach to AI

By Mauritz Kop[1]

On 21 April 2021, the European Commission presented the Artificial Intelligence Act. As a Fellow at Stanford University's Transatlantic Technology Law Forum and a Member of the European AI Alliance, I made independent strategic recommendations to the European Commission. President Ursula von der Leyen's team adopted some of the suggestions that I offered them, or has itself arrived to the same conclusions. That is encouraging. This contribution will list the main points of this novel regulatory framework for AI.

Core horizontal rules for AI

The EU AI Act sets out horizontal rules for the development, commodification and use of AI-driven products, services and systems within the territory of the EU. The draft regulation provides core artificial intelligence rules that apply to all industries. The EU AI Act introduces a sophisticated 'product safety framework' constructed around a set of 4 risk categories . It imposes requirements for market entrance and certification of High-Risk AI Systems through a mandatory CE-marking procedure. To ensure equitable outcomes, this pre-market conformity regime also applies to machine learning training, testing and validation datasets. The Act seeks to codify the high standards of the EU trustworthy AI paradigm, which requires AI to be legally, ethically and technically robust, while respecting democratic values, human rights and the rule of law.

Objectives of the EU Artificial Intelligence Act

The proposed regulatory framework on Artificial Intelligence has the following objectives:

1. ensure that AI systems placed on the Union market and used are safe and respect existing law on fundamental rights and Union values;

2. ensure legal certainty to facilitate investment and innovation in AI;

3. enhance governance and effective enforcement of existing law on fundamental rights and safety requirements applicable to AI systems;

[1] Mauritz Kop is Stanford Law School TTLF Fellow at Stanford University and is Managing Partner at AIRecht, Amsterdam, The Netherlands.

4. facilitate the development of a single market for lawful, safe and trustworthy AI applications and prevent market fragmentation.

Subject Matter of the EU AI Act

The scope of the AI Act is largely determined by the subject matter to which the rules apply. In that regard, Article 1 states that:

Article 1
Subject matter

This Regulation lays down:

(a) harmonised rules for the placing on the market, the putting into service and the use of artificial intelligence systems ('AI systems') in the Union;

(a) prohibitions of certain artificial intelligence practices;

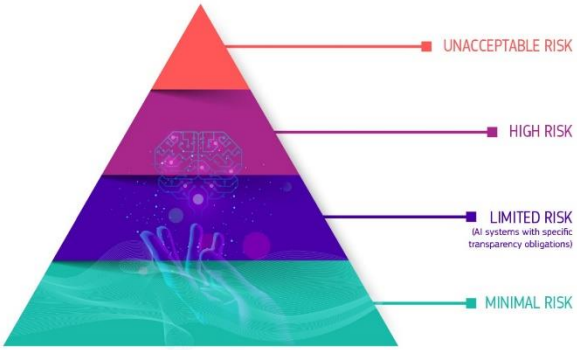
(b) specific requirements for high-risk AI systems and obligations for operators of such systems;

(c) harmonised transparency rules for AI systems intended to interact with natural persons, emotion recognition systems and biometric categorisation systems, and AI systems used to generate or manipulate image, audio or video content;

(d) rules on market monitoring and surveillance.

Pyramid of Criticality: Risk based approach

To achieve the goals outlined, the Artificial Intelligence Act draft combines a risk-based approach based on the pyramid of criticality, with a modern, layered enforcement mechanism. This means, among other things, that a lighter legal regime applies to AI applications with a negligible risk, and that applications with an unacceptable risk are banned. Between these extremes of the spectrum, stricter regulations apply as risk increases. These range from non-binding self-regulatory soft law impact assessments accompanied by codes of conduct, to heavy, externally audited compliance requirements throughout the life cycle of the application.



The Pyramid of Criticality for AI Systems

Unacceptable Risk AI systems

Unacceptable Risk AI systems can be divided into 4 categories: two of these

concern cognitive behavioral manipulation of persons or specific vulnerable groups. The other 2 prohibited categories are social scoring and real-time and remote biometric identification systems. There are, however, exceptions to the main rule for each category. The criterion for qualification as an Unacceptable Risk AI system is the harm requirement.

Examples of High-Risk AI-Systems

Hi-Risk AI-systems will be carefully assessed before being put on the market and throughout their lifecycle. Some examples include:

- *Critical infrastructures (e.g. transport), that could put the life and health of citizens at risk*
- *Educational or vocational training, that may determine the access to education and professional course of someone's life (e.g. scoring of exams)*
- *Safety components of products (e.g. AI application in robot-assisted surgery)*
- *Employment, workers management and access to self-employment (e.g. CV sorting software for recruitment procedures)*
- *Essential private and public services (e.g. credit scoring denying citizens opportunity to obtain a loan)*
- *Law enforcement that may interfere with people's fundamental rights (e.g. evaluation of the reliability of evidence)*
- *Migration, asylum and border control management (e.g. verification of authenticity of travel documents)*
- *Administration of justice and democratic processes (e.g. applying the law to a concrete set of facts)*
- *Surveillance systems (e.g. biometric monitoring for law enforcement, facial recognition systems)*

Market Entrance of High-Risk AI-Systems: 4 Steps

In a nutshell, these 4 steps should be followed prior to Hi-Risk AI-Systems market entrance. Note that these steps apply to components of such AI systems as well.

1. A High-Risk AI system is developed, preferably using internal ex ante AI Impact Assessments and Codes of Conduct overseen by inclusive, multidisciplinary teams.

2. The High-Risk AI system must undergo an approved conformity assessment and continuously comply with AI requirements as set forth in the EU AI Act, during its lifecycle. For certain systems an external notified body will be involved in the conformity assessment audit. This dynamic process ensures benchmarking, monitoring and validation. Moreover, in case of changes to the High-Risk AI system, step 2 has to be repeated.

3. Registration of the stand-alone Hi-Risk AI system will take place in a dedicated EU database.

4. A declaration of conformity must be signed and the Hi-Risk AI system must carry the CE marking (Conformité Européenne). Now the system is ready to enter the European markets.

But this is not the end of the story...

In the vision of the EC, after the Hi-Risk AI system haven obtained market approval, authorities on both Union and Member State level '*will be responsible for market surveillance, end users ensure monitoring and human oversight, while providers have a post-market monitoring system in place. Providers and users will also report serious incidents and malfunctioning.*' [2] In other words, continuous upstream and downstream monitoring.

Since people have the right to know if and when they are interacting with a machine's algorithm instead of a human being, the AI Act introduces specific transparency obligations for both users and providers of AI system, such as bot disclosure. Likewise, specific transparency obligations apply to automated emotion recognition systems, biometric categorization and deepfake/synthetics disclosure. Limited Risk AI Systems such as chatbots necessitate specific transparency obligations as well. The only category exempt from these transparency obligations can be found at the bottom of the pyramid of criticality: the Minimal Risk AI Systems.

In addition, natural persons should be able to oversee the Hi-Risk AI-System. This is termed the human oversight requirement.

Open Norms

The definition of high-risk AI applications is not yet set in stone. Article 6 does provide classification rules. Presumably, the qualification remains a somewhat open standard within the regulation, subject to changing societal views, and to be interpreted by the courts, ultimately by the EU Court of Justice. A standard that is open in terms of content and that needs to be fleshed out in more detail under different circumstances, for example using a catalog of viewpoints. Open standards entail the risk of differences of opinion about their interpretation. If the legislator does not offer sufficient guidance, the courts will ultimately have to make a decision about the interpretation of a standard. This can be seen as a less desirable side of regulating with open standards. A clear risk taxonomy will contribute to legal certainty and offer stakeholders with appropriate answers to questions about liability and insurance.

Enforcement

[2] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/excellence-trust-artificial-intelligence_en

The draft regulation provides for the installation of a new enforcement body at Union level: the European Artificial Intelligence Board (EAIB). At Member State level, the EAIB will be flanked by national supervisors, similar to the GDPR's oversight mechanism. Fines for violation of the rules can be up to 6% of global turnover, or 30 million euros for private entities.

'*The proposed rules will be enforced through a governance system at Member States level, building on already existing structures, and a cooperation mechanism at Union level with the establishment of a European Artificial Intelligence Board.*'[3]

CE-marking: pre-market conformity requirements

In line with my recommendations, Article 49 of the Artificial Intelligence Act requires high-risk AI and data-driven systems, products and services to comply with EU benchmarks, including safety and compliance assessments. This is crucial because it requires products and services to meet the high technical, legal and ethical standards that reflect the core values of trustworthy AI. Only then will they receive a CE marking that allows them to enter the European markets. This pre-market conformity & legal compliance mechanism works in the same manner as the existing CE marking: as safety certification for products traded in the European Economic Area (EEA).

Please note that this pre-market conformity regime also applies to machine learning training, testing and validation datasets on the basis of article 10. These corpora need to be representative (I would almost say: inclusive), hi- quality, adequately labelled and error-free to ensure non-discriminatory and non-biased outcomes. Thus, the input data must abide to the high standards of trustworthy AI as well.

Pursuant to Article 40, harmonized standards for high-risk AI systems are published in the Official Journal of the European Union:

Article 40
Harmonised standards

High-risk AI systems which are in conformity with harmonised standards or parts thereof the references of which have been published in the Official Journal of the European Union shall be presumed to be in conformity with the requirements set out in Chapter 2 of this Title, to the extent those standards cover those requirements.

The CE marking for the individual types of high-risk AI systems can be applied for via a procedure as described in article 43.

Article 43
Conformity assessment

1. For high-risk AI systems listed in point 1 of Annex III, where, in demonstrating the

[3] ibid

compliance of a high-risk AI system with the requirements set out in Chapter 2 of this Title, the provider has applied harmonised standards referred to in Article 40, or, where applicable, common specifications referred to in Article 41, the provider shall follow one of the following procedures:

(a)the conformity assessment procedure based on internal control referred to in Annex VI;

(b)the conformity assessment procedure based on assessment of the quality management system and assessment of the technical documentation, with the involvement of a notified body, referred to in Annex VII.

Where, in demonstrating the compliance of a high-risk AI system with the requirements set out in Chapter 2 of this Title, the provider has not applied or has applied only in part harmonised standards referred to in Article 40, or where such harmonised standards do not exist and common specifications referred to in Article 41 are not available, the provider shall follow the conformity assessment procedure set out in Annex VII.

For the purpose of the conformity assessment procedure referred to in Annex VII, the provider may choose any of the notified bodies. However, when the system is intended to be put into service by law enforcement, immigration or asylum authorities as well as EU institutions, bodies or agencies, the market surveillance authority referred to in Article 63(5) or (6), as applicable, shall act as a notified body.

...

Article 43 paragraph 6 aims to prevent or avoid risks with regard to health, safety and fundamental rights:

6. The Commission is empowered to adopt delegated acts to amend paragraphs 1 and 2 in order to subject high-risk AI systems referred to in points 2 to 8 of Annex III to the conformity assessment procedure referred to in Annex VII or parts thereof. The Commission shall adopt such delegated acts taking into account the effectiveness of the conformity assessment procedure based on internal control referred to in Annex VI in preventing or minimizing the risks to health and safety and protection of fundamental rights posed by such systems as well as the availability of adequate capacities and resources among notified bodies.

Article 48 paragraph 1, EU declaration of conformity indicates that:

Article 48
EU declaration of conformity

1.The provider shall draw up a written EU declaration of conformity for each AI system and keep it at the disposal of the national competent authorities for 10 years after the AI system has been placed on the market or put into service. The EU declaration of conformity shall identify the AI system for which it has been drawn up. A copy of the EU declaration of conformity shall be given to the

relevant national competent authorities upon request.

...

Further, Article 49 CE marking of conformity determines that:

Article 49
CE marking of conformity

1.The CE marking shall be affixed visibly, legibly and indelibly for high-risk AI systems. Where that is not possible or not warranted on account of the nature of the high-risk AI system, it shall be affixed to the packaging or to the accompanying documentation, as appropriate.

2.The CE marking referred to in paragraph 1 of this Article shall be subject to the general principles set out in Article 30 of Regulation (EC) No 765/2008.

3.Where applicable, the CE marking shall be followed by the identification number of the notified body responsible for the conformity assessment procedures set out in Article 43. The identification number shall also be indicated in any promotional material which mentions that the high-risk AI system fulfils the requirements for CE marking.

Finally, Article 30 of the draft regulation on notifying authorities provides that:

Article 30
Notifying authorities

1.Each Member State shall designate or establish a notifying authority responsible for setting up and carrying out the necessary procedures for the assessment, designation and notification of conformity assessment bodies and for their monitoring.

2.Member States may designate a national accreditation body referred to in Regulation (EC) No 765/2008 as a notifying authority.

3.Notifying authorities shall be established, organised and operated in such a way that no conflict of interest arises with conformity assessment bodies and the objectivity and impartiality of their activities are safeguarded.

...

Self assessment too non-committal (non-binding)?

First, it is crucial that certification bodies and notified bodies are independent and that no conflicts of interest arise due to a financial or political interest. In this regard, I wrote elsewhere that the EU should be inspired by the modus operandi of the US FDA.

Second, the extent to which companies can achieve compliance with this new AI 'product safety regime' through risk-based self-assessment and self-certification, without third party notified bodies, determines the effect of the Regulation on business practices and thus on the preservation and reinforcement of our values. Internally audited

self-assessment is too non-committal given the high risks involved. Therefore, I think it is important that the final version of the EU AI Act subjects all high-risk systems to external, independent third party assessments requirements. Self-regulation in combination with awareness of the risks via (voluntary or mandatory) internal ai impact assessments is not enough to protect our societal values, since companies have completely different incentives for promoting social good and pursuing social welfare, than the state. We need mandatory third party audits for all High-Risk AI Systems.

In this regard, it is interesting to compare the American way of regulating AI with the European approach. In America people tend to advocate free market thinking and a laissez faire approach. For example, the Stanford University, Silicon Valley group The Adaptive Agents Group recently proposed The Shibboleth Rule for Artificial Agents. Their proposal is reminiscent of the EU Human oversight requirement, and maintains that:

'Any artificial agent that functions autonomously should be required to produce, on demand, an AI shibboleth: a cryptographic token that unambiguously identifies it as an artificial agent, encodes a product identifier and, where the agent can learn and adapt to its environment, an ownership and training history fingerprint.'[4]

Their modest proposition contrasts strongly with the widely scoped European legal-ethical framework. However, history has already taught us dramatically that the power and social impact of AI is too great to be left largely to the companies themselves.

In addition, it is key that international standard setting bodies like ISO and IEEE adopt and translate the norms and values of the EU Act in their own technical standards, so that they are in line with each other. Such harmonized standards will encourage sustainable innovation and responsible business practices. In other words, worldwide adoption of such technical standards increases the chance that leading firms will adjust their behavior vis-a-vis AI.

Moreover, a harmonized global framework prevents forum shopping. With forum shopping I mean finding the most favorable possible regime to achieve one's own rights, motivated by financial interests that are often at the expense of consumers, competition, the environment and society.

Innovation Friendly Flexibilities: Legal Sandboxes

In line with my recommendations, the draft aims to prevent the rules from stifling innovation and hindering the creation of a flourishing AI ecosystem in Europe. This is ensured by introducing various flexibilities and exceptions, including the application of legal sandboxes that afford breathing room to research institutions and SME's. Thus, to guarantee room for innovation, the draft establishes AI regulatory sandboxes. Further, an IP Action Plan has been drawn up to

[4] https://hai.stanford.edu/news/shibboleth-rule-artificial-agents

modernize technology related intellectual property laws.

'Additional measures are also proposed to support innovation, in particular through AI regulatory sandboxes and other measures to reduce the regulatory burden and to support Small and Medium-Sized Enterprises ('SMEs') and start-ups.'[5]

The concept thus seeks to balance divergent interests, including democratic, economic and social values. That irrevocably means that trade-offs will be made. It is to be hoped that during its journey through the European Parliament, the proposal will not be relegated to an unworkable compromise, as happened recently with the Copyright Directive, under the influence of the lobbying power of a motley crew of stakeholders.

Sustainability

Moreover, the explanatory memorandum pays attention to the environment and sustainability, in the sense that the ecological footprint of technologies should be kept as small as possible and that the application of artificial intelligence should support socially and environmentally beneficial outcomes. This is in line with article 37 of the EU Charter of Fundamental Rights ('the Charter'), and the EU Green Deal, which strives for the decarbonization of our society.

Sector specific rules

On top of the new AI rules, AI infused systems, products and services must comply with sector-specific regulations such as the Machinery Directive and the Regulations for medical devices (MDR) and in vitro diagnostics (IVDR), as well. Furthermore, besides the General Data Protection Regulation (GDPR) for personal data, the FFD Regulation for non-personal data and both GDPR and FFD for mixed datasets, the upcoming Data Act will apply. This applies, among other things, to B2B and B2G data sharing (depending on the types of data used), the use of privacy-preserving synthetic dataset generation techniques, and the use of machine learning training and validation data sets. In addition, audits of products and services equipped with AI must fit into existing quality management systems of industries and economic sectors such as logistics, energy and healthcare.

Regulations versus Directives

In the EU, regulations result in unification, in unification of legal rules. Member States have no discretion here for their own interpretation of the Brussels regulations. Member States do have that room for directives. Directives on the other hand, lead to harmonization of legal rules. Regulations such as the new Artificial Intelligence Act are directly applicable in the national legal orders of the member states, without the need for transposition or implementation. As was necessary, for example, with the recent Copyright Directive. As soon as the European

[5] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/excellence-trust-artificial-intelligence_en

Parliament and the Council of Europe agree with the final text in mid-2022 and if it is adopted, the AI Regulation will be immediately applicable law in all countries of the European Union.

AI Governance: trans-Atlantic perspectives

It is understandable that the European Union considers AI to be part of European strategic autonomy. Moreover, a degree of strategic European digital sovereignty is needed to safeguard European culture. Nevertheless, it is of existential importance for the EU to work together in concert with countries that share our European digital DNA, based on common respect for the rule of law, human rights and democratic values. Against this background, it is essential to stimulate systematic, multilateral transatlantic cooperation and jointly promote and achieve inclusive, participatory digitalization. The transatlantic and geopolitical dialogue on transformative technology, together with the development of globally accepted technology standards and protocols for interoperability, should be strengthened.

Setting Global Standards for AI

It takes courage and creativity to legislate through this stormy, interdisciplinary matter, forcing US and Chinese companies to conform to values-based EU standards before their AI products and services can access the European market with its 450 million consumers. Consequentially, the proposal has extraterritorial effect.

By drafting the Artificial Intelligence Act and embedding our norms and values into the architecture and infrastructure of our technology, the EU provides direction and leads the world towards a meaningful destination. As the Commission did before with the GDPR, which has now become the international blueprint for privacy, data protection and data sovereignty.

Methods also useful for other emerging technologies

While enforcing the proposed rules will be a whole new adventure, the novel legal-ethical framework for AI enriches the way of thinking about regulating the Fourth Industrial Revolution (4IR). This means that - if proven to be useful and successful - we can also use methods from this legal-ethical cadre for the regulation of 4IR technologies such as quantum technology, 3D printing, synthetic biology, virtual reality, augmented reality and nuclear fusion. It should be noted that each of these technologies requires a differentiated horizontal-vertical legislative approach in terms of innovation incentives and risks.

Trustworthy AI by Design

Responsible, Trustworthy AI requires awareness from all parties involved, from the first line of code. The way in which we design our technology is shaping the future of our society. In this vision democratic

values and fundamental rights play a key role. Indispensable tools to facilitate this awareness process are AI impact and conformity assessments, best practices, technology roadmaps and codes of conduct. These tools are executed by inclusive, multidisciplinary teams, that use them to monitor, validate and benchmark AI systems. It will all come down to *ex ante* and life-cycle auditing.

The new European rules will forever change the way AI is formed. Pursuing trustworthy AI by design seems like a sensible strategy, wherever you are in the world.

Other Developments

European Union

EU Digital Consumer Contract Law – The Directive on Contracts for the Supply of Digital Content and Digital Services

By Sebastian Pech

The Directive (EU) 2019/770 on Contracts for the Supply of Digital Content and Digital Services governs the relationship between traders and consumers within this context, and will apply from January 1, 2022. The Directive's scope of application is broad and affects many types of contracts. This contribution provides an overview of the new regulations.

1. Background of the Directive

The Directive is intended to ensure a high level of consumer protection and legal certainty in cross-border transactions involving digital content and services (see Recitals 4–11). Therefore, the Directive follows the principle of full harmonization, which means that regulations that are introduced by the Member States should meet its threshold, and should not be exceedingly stringent or lenient (Article 4). Furthermore, the regulations set forth in the Directive are of a mandatory nature. Therefore, contractual terms between traders and consumers that differ in a way that is detrimental to the consumer are not binding for the consumer (Article 22).

The member states had to enact the Directive into national law by July 1, 2021, and the new regulations will come into force on January 1, 2022 (Article 24).

2. Scope of Application

a. Material Scope

The material scope of the Directive relates to digital content and digital services:

- **Digital content** means "data which are produced and supplied in digital form" (Article 2 (1)). This includes computer programs, games, music, videos, and texts in digital form, regardless of whether they are provided in a physical medium (e.g., CD, DVD, USB stick), as a download, or on a stream (Recital 19). The supply of digital content can occur through a single act (e.g., a file that is downloaded to the consumer's device, through which the consumer has indefinite access) or on an ongoing basis for a specified period (e.g., a movie on a streaming platform, for which the consumer has access only during the term of the contract) (Recitals 56, 57).

- **Digital services** comprise services "that allow[…] the consumer to create, process, store or access data in digital form" as well as services "that allow[…] the sharing of or any other interaction with data in digital form, [which are] uploaded or created by the consumer or other users of that service" (Article 2 (2)). Examples of digital services are cloud storage, messenger services, online games, and social networks (Recital 19).

The definitions of digital content and digital services are intentionally broad, to cover future technical developments (Recitals 10, 19). In practice, it is not always possible to distinguish between digital content and digital services clearly. In most cases, however, this distinguishment is unnecessary, as both categories are primarily treated in the same way.

The Directive is not only applicable to contracts in which the consumer pays money to the trader, but also when the consumer provides personal data that is processed by the trader (Article 3 (1)). The only exception is if personal data are used exclusively by the trader for contractual performance (e.g., requesting an email address because the contract is performed via e-mail) or due to a legal obligation (e.g., originating from a tax law). In practice, "paying with data" is used specifically for contracts on social networks.

b. Personal Scope

Regarding the personal scope of the Directive, the contract must be concluded between a trader and consumer (B2C). Contracts between businesses (B2B) are not covered.

3. Obligation of the Trader to Supply Digital Content or Service to the Consumer

a. Extent of the obligation

The trader has an obligation to supply the digital content or service to the consumer by making it accessible or available to them (Article 5). However, transmission to the consumer is not required, so the trader's obligation is fulfilled as soon as the consumer can use the digital content or service, without any further action required by the trader (Recital 41).

If no time of performance has been agreed on by the parties, the trader must provide the digital content or service without undue delay after the conclusion of the contract (Article 5 (1)).

b. Burden of Proof

The burden of proof regarding whether the digital content or service was supplied in time is on the trader.

c. Remedies

In case the trader fails to supply the digital content or service to the consumer in time, the consumer is entitled to terminate the contract, after having unsuccessfully requested the trader to provide the content or service (Article 13 (1)). In certain cases, the

consumer's request is not required, for example, if the trader refuses to provide the content or service (Article 13 (2)).

In the event of termination of the contract, the trader must reimburse the consumer for any payments already made (Articles 13 (3), 16 (1)).

4. Obligation of the Trader to Supply Digital Content or Service to the Consumer in Conformity with the Contract

Furthermore, the trader has an obligation to supply the digital content or service to the consumer, in conformity with the contract (Article 6).

a. Extent of the obligation

Conformity with the contract requires that the digital content or service meets subjective and objective requirements, is integrated correctly, and does not infringe on the rights of third parties (Article 6):

- **Subject requirements** for conformity result from an agreement between the trader and consumer (Article 7).
- **Objective requirements** are determined by the circumstances of the contract and the nature of the digital content or service involved. These factors are, in particular, (a) whether the digital content or service is fit for its usual purpose, or (b) whether it possesses the usual quality for content or services of its same type, and based on what the consumer can reasonably expect, given the nature of the content or service (Article 8 (1)). The usual quality includes requirements that result from public statements (e.g., advertising statements) of the trader and/or developer of the digital content or service.

The trader may deviate from the objective requirements by agreement with the consumer. However, strict requirements are placed on such an agreement. The trader must inform the consumer specifically as to the deviations from the objective requirements, at the time of the conclusion of the contract, and the consumer must expressly and separately accept these deviations (Article 8 (5)).

- A lack of conformity to the contract can also result from an **incorrect integration** of the digital content or service into the consumer's digital environment by the trader, or by the consumer, due to shortcomings in the integration instructions provided by the trader (Article 9).
- Finally, conformity to the contract requires that the use of the digital content or service does not **violate the rights of third parties**, especially intellectual property rights (Article 10).

The relevant point in time when the content or service must conform to the contract is determined by the type of supply:

- Where a contract provides for a **single act of supply,** the content or service

must comply with the contract at the time of supply (Article 11 (2)).

- In the case of a **continuous supply over a specific period,** the content or service must conform to the contract during the entire period that it is supplied to the consumer (Article 8 (4), 11 (3)).

b. Burden of Proof

In general, the burden of proof on whether the digital content or service was supplied in conformity to the contract is on the consumer (Recital 59). However, to protect the consumer, burden of proof is shifted to the trader in certain instances. Here too, a distinction is made according to the type of supply:

- Where a contract provides for a **single act of supply,** the burden of proof regarding whether the supplied digital content or service conforms to the contract at the time of supply is on the trader if it is within one year from the time when the digital content or service was supplied (Article 12 (2)).

- In the case of a **continuous supply over a specific period,** the burden of proof regarding whether the digital content or service conforms to the contract within the period of supply is on the trader (Article 12 (3)).

c. Remedies

If the digital content or service is not provided to the consumer in conformity with the contract, the consumer is entitled to have the digital content or service brought into conformity with the contract, to receive a reduction in the price, or to terminate the contract (Article 14 (1)):

- If the consumer demands to **have the content or service brought into conformity,** the trader must comply with this demand within a reasonable period, and at his own cost, unless bringing the content or service into conformity will be impossible or can only be carried out at disproportionate costs (Article 14 (2), (3)).

It is left to the discretion of the trader to decide how to bring the content or service into conformity; for example, by providing a new copy of the content or service to the consumer, or by issuing an update of it (Recital 63). However, often in practice, it is not simply the individual digital content or service being supplied to the consumer that lacks conformity, but the entire series (e.g., software version); therefore, providing a new copy to the consumer will be insufficient. In addition, updating the digital content or service will often be impossible or disproportionately costly for the trader if they are not the developer of the digital content or service. Therefore, the Directive leaves it up to the member states to introduce a direct claim from the consumer against the developer of the digital content or service (Recital 13).

- If certain conditions are complied with, for example, when it is impossible or refused by the trader to bring the contract into conformity, the consumer can

demand a proportionate **reduction of the price** (Article 14 (4), (5)). However, when "paying with data," such a reduction is excluded.

- Instead of demanding to reduce the price, the consumer may also **terminate** the contract. If the lack of conformity is only minor, termination of the contract is not possible (Article 14 (6)) unless the consumer "pays with data" (Recital 67).

Similar to the termination of the contract due to a failure to supply the digital content or service in time, the trader must reimburse the consumer for payments already made. However, in the case of continuous supply over a specific period, reimbursement will occur only for the time during which the digital content or service was not in conformity with the contract (Article 16 (1)).

After termination of the contract, the consumer may not continue to use the digital content or service or make it available to third parties (Article 17 (1)). In practice, this will not always be easy to control. If digital content was provided on a physical medium, the consumer is obligated to return it at the request and expense of the trader (Article 17 (2)). However, the trader may also actively prevent the consumer's ability to use the digital content or service; for example, this can be done by disabling the user's account or through technical measures (Article 16 (5)).

Inversely, if the consumer has created or supplied the trader with digital content (e.g., user-generated content), the trader must refrain from using that content after termination of the contract and must make it available to the consumer upon request (Article 16 (3), (4)). However, in most cases, the content created or provided by the consumer will be personal data; hence, the General Data Protection Regulation (GDPR) is applicable, and not the Directive on digital content and services (Recital 38).

5. Updates and Other Modifications of Digital Content and Service

a. Updates

The trader must provide updates that are necessary to maintain the conformity of the digital content or service with the contract (e.g., security updates) and inform the consumer thereof (Article 8 (2)). This applies not only to contracts on the continuous supply of digital content or services over a specific period, but also for a single act of supply.

The relevant duration for providing updates is determined by the type of supply:

- In the case of a **continuous supply over a specific period,** the obligation to update runs for the entire contract term (Article 8 (2) (a)).

- Where a contract provides for a **single act of supply,** the period depends on how long the consumer can reasonably expect updates to be provided (Article 8 (2) (a)). Factors to be considered here are the type and purpose of the digital

content or service, the circumstances, and the nature of the contract.

The Directive does not establish an independent obligation on the trader to provide updates to the consumer, but instead treats updates as a subset of the obligation to supply the digital content or service to the consumer, in conformity with the contract. Therefore, if the trader fails to provide updates, the content or service will fall short of the objective requirements for conformity. As a result, the consumer can *inter alia* demand to have the content or service brought into conformity by the trader (Article 14 (2), (3)). However, updating the digital content or service will often be impossible or disproportionately expensive for the trader if they are not the developer of the digital content or service. In practice, if there is no direct claim against the developer of the content or service, the consumer has only the option of demanding a reduction of the price or terminating the contract with the trader.

b. Other Modifications

In the case of continuous supply over a specific period, the trader may have an interest in modifying the content or service, without the necessity to maintain conformity with the contract. This applies, for example, to a software's range of features or the content available on an audio or video streaming platform. Such modifications require that: (a) the contract allows and provides for a valid reason regarding the modification, (b) the modification is made without additional cost to the consumer, and (c) the consumer is informed, in a clear and comprehensible manner, regarding the modification (Article 19 (1) (a)–(c)). These requirements apply to all modifications, regardless of whether they are favorable or unfavorable to the consumer (see Recital 75). However, if the modification negatively impacts the consumer's access to or use of the digital content or service, the consumer must be informed reasonably and in advance of the features and time of such modification (Article 19 (1) (d)). In addition, the consumer must also be notified of their right to terminate the contract (Article 19 (2)) and the possibility of keeping the digital content or service without modification (Article 19 (4)).

6. Right of Redress

If the trader is liable to compensate a consumer because of a failure to supply the digital content or service, or a lack of contract conformity of the digital content or service, and such issue was caused by a person in the supply chain (e.g., the developer), the trader is entitled to remedies against that person (Article 20).

7. Aspects Not Covered by the Directive

The Directive does not cover aspects of general contract law, such as the formation or validity of a contract on the supply of digital content or digital service (Article 3 (10). Furthermore, no classification is made as to the legal nature of contracts for digital content or service for example, these could be in the form of sales, rentals, or *sui generis*

contracts (Recital 12). Furthermore, the Directive does not contain any provisions regarding the consumer's right to damages in the case of failure to supply digital content or services and in the event of lack of conformity to the contract (Article 3 (10)). Finally, the question of what occurs if the consumer exercises their rights, as set forth in the GDPR (i.e., to withdraw consent to the processing of personal data) is not addressed (Recital 40). This becomes particularly relevant when the consumer “pays with data.”

The issues that are not covered by the Directive can be regulated by the member states, at their own discretion.

8. Conclusion

The Directive establishes specific regulations for consumer contracts regarding digital content and services. These apply not only to contracts where the consumer pays a price, but also when they provide personal data to the trader.

The Directive leaves not only certain aspect to be regulated by the Member States, but also specific aspects to be clarified by the courts, such as the question regarding the duration of the trader’s obligation to update, for contracts of a single act of supply.

It is also uncertain whether, in practice, consumers will be able to enforce the rights that they are entitled to, particularly regarding claims against the trader to have brought the content or service into conformity if the trader is not the developer of the digital content or service.

Therefore, it remains to be seen whether the new regulations will achieve the goal of the Directive: to ensure a high level of consumer protection and legal certainty in cross-border transactions involving digital content and services.

Other Developments
European Union

CJEU: Intra-EU Investor-State Arbitration under the Energy Charter Treaty is not Compatible with EU Law

By Gabriel M. Lentner and Dayana Zasheva

On 2 September 2021, the Court of Justice of the European Union (CJEU) delivered its preliminary ruling in *Moldova v. Komstroy LLC*, holding that intra-EU investor-State arbitrations under the Energy Charter Treaty (ECT) are incompatible with EU law.

Background

On 25 October 2013, a Paris-seated arbitral tribunal, constituted under Article 26 ECT, found Moldova liable to pay damages to the Ukrainian investor Energoalians (whose successor later became Komstroy) for violations of the ECT. Moldova sought to set aside the award on the basis of a lack of jurisdiction. The Paris Court of Appeal was therefore confronted with the question of what types of investments are covered by the ECT and decided to refer this issue to the CJEU.

Most important and although no EU parties were involved in the arbitration itself, the European Commission and several EU Member States seized this case as an opportunity to ask the CJEU also to rule on whether intra-EU investor-State arbitration under the ECT is incompatible with EU law.

CJEU has jurisdiction over the matter

The CJEU's jurisdiction was questioned on the ground that the disputed arbitral award did not involve parties to the EU. However, the CJEU held that the conclusion of the ECT by the Council constitutes an act of the EU institutions and thus the CJEU can interpret it as such pursuant to Article 267 TFEU (paras 22-23). The CJEU also underlined that the parties, by selecting Paris as the seat of arbitration, have chosen the French law as *lex fori*, which necessarily entails the application of EU law (paras 33-34).

Intra-EU investor-State arbitration under ECT is contrary to EU law

On the question of compatibility, the CJEU first stated that an intra-EU investor-State arbitration under the ECT will inevitably involve application of EU law, as the conclusion of the ECT by the Council is an act of EU law (paras 49-50).

Second, the CJEU noted that an ad hoc tribunal under Article 26 ECT is, however, not a part of the EU judicial system (paras 52-53). Therefore, it is not entitled to make a reference for a preliminary ruling under Article 267 TFEU. This was found to lead to a removal from the judicial system of disputes concerning EU law which undermines the full effectiveness and uniform interpretation of EU rules as held in the now well-known *Achmea* decision (para 60-61).

Third, the CJEU held that a domestic law provision allowing a limited review of the arbitral award is not sufficient to meet the obligation of Member States under Article 19(1) TEU to provide sufficient remedies in the areas covered by EU law (paras 57-59).

Lastly, the CJEU ruled that the fact that the EU itself has concluded the ECT cannot render the intra-EU investor-State arbitration provided for therein compatible with EU law (para 62).

Conclusion

The finding that ECT investor-State arbitration in intra-EU disputes is incompatible with EU law was to be expected in view of previous CJEU decisions. Accordingly, the *Achmea* decision, which put an end to investor-State arbitration clauses in BITs between Member States, and *Opinion 2/13*, which blocked EU's accession to the European Convention on Human Rights due to incompatibility with the principle of autonomy, paved the way for it.

Moreover, this decision was foreshadowed by EU's initiatives such as the Agreement for the Termination of BITs between the Member States and the EU's proposal to modernize the ECT by establishing a multilateral investment court applicable to disputes under the ECT. [6]

It will be interesting to see whether the CJEU will follow this line of reasoning and find individual intra-EU investor-State arbitration agreements also incompatible with EU law – a question pending for a preliminary ruling in the *PL Holdings* case.

[6] Clement Fouchard and Vanessa Thieffry, 'CJEU Ruling in Moldova v. Komstroy: the End of Intra-EU Investment Arbitration Under the Energy Charter Treaty (and a Restrictive Interpretation of the Notion of Protected Investment)' (7 September 2021) Kluwer Arbitration Blog.

Other Developments
European Union

Investor-State Dispute Settlement and EU law: Opinion of the Advocate General on Individual Arbitration Agreements

By Gabriel M. Lentner and Dayana Zasheva

On 22 April 2021, the Advocate General Kokott issued her opinion in Case C-109/20 on whether Articles 267 and 344 TFEU as interpreted in the judgement in *Achmea* allow individual arbitration agreements between an EU investor and a Member State.

Background

The preliminary question concerns the validity under EU law of the arbitral award between Poland and the investor PL Holdings issued under the BLEU-Poland BIT on 28 September 2017. In the arbitral proceedings, Poland objected to the jurisdiction of the tribunal by claiming that the arbitration clause was invalid under EU law. However, the objection was found belated and, thus, inadmissible (para 15). As a result, Poland was ordered to pay EUR 150 million in damages to the investor PL Holdings for ordering it to divest its shares in a Polish bank (para 17).

Subsequently, Poland brought an action before the Swedish courts to set aside the PL Holdings award. Poland claimed that the arbitration clause of the BLEU-Poland BIT was invalid as it infringed EU law. The Stockholm Court of Appeal accepted that *Achmea* rendered Poland's consent to arbitration contained in the applicable BLEU-Poland BIT invalid. However, since Poland's objection to the tribunal's jurisdiction was raised belatedly, the court found that an individual arbitration agreement was concluded with the investor. The Stockholm Court therefore refused to set aside the contested award (para 19).

Unsatisfied, Poland appealed these findings to the Supreme Court of Sweden. On 4 February 2020, the Supreme Court of Sweden requested a preliminary ruling from the CJEU asking the following question:

'Do Articles 267 and 344 TFEU, as interpreted in *Achmea*, mean that an arbitration agreement is invalid if it has been concluded between a Member State and an investor — where an investment agreement contains an arbitration clause that is invalid as a result of the fact that the contract was concluded between two Member States — [despite the fact that] the Member State, after arbitration proceedings were commenced by the investor, refrains, by the free will of

the State, from raising objections as to jurisdiction?'

The Opinion of the Advocate General on the question requires consideration as its aimed to assist the CJEU in its response and the CJEU generally follows it.

Arbitration between an investor and a Member State is permissible provided that it can be comprehensively reviewed for compliance with EU law

In answering the Swedish Supreme Court's question, the Advocate General began by recalling the *Achmea* judgement, which held that Articles 267 and 344 TFEU preclude investor-State arbitral clauses between Member States. According to the Advocate General the reason for the ruling in *Achmea* was the reference of EU law disputes to bodies which cannot refer to the CJEU for a preliminary ruling under Article 267 TFEU (para 30). For the Advocate General, this threatens the full effect, consistency and autonomy of EU law and is a violation of Article 344 TFEU (para 26). Under this provision Member States are to ensure the application of EU law by submitting disputes concerning EU law exclusively to the settlement mechanism provided for in the Treaties (para 27).

The Advocate General proceeded by examining whether the concerns in *Achmea* will render the investment agreements between an investor and a Member State also invalid.

First, the Advocate General noted that the dispute concerned EU law. While the PL Holdings tribunal did not directly apply EU law provisions, it nevertheless examined whether Poland complied with EU standards, such as proportionality, when exercising the banking supervision (para 33). In any case, the Advocate General held that EU law inevitably was part of the dispute, as it formed part of the Polish law (para 38).

Second, the Advocate General noted that the PL Holdings arbitral tribunal is not part of the EU judicial system (para 36). Therefore, it is not entitled to make a reference for a preliminary ruling under Article 267 TFEU in respect of doubts about the interpretation of EU law (para 35). This, according to the Advocate General, leads to removal of EU law disputes from the EU judicial system (paras 34-36). Such a removal renders the arbitration agreement between an investor and a Member State incompatible with Articles 267 and 344 TFEU pursuant to the *Achmea* judgement (paras 34-36). Specifically, in such cases, the Advocate General considered that the autonomy of EU law is threatened (para 37) and there is a risk that the arbitral award may be in breach of EU law (para 38) and lead to aprecedent that the courts of the Member States could follow (39).

The Advocate General held that in any event the risk of the infringement of EU law could be countered if the Member States can comprehensively examine whether the award complies with EU law and, if necessary, refer the matter for a preliminary ruling under Article 267 TFEU (para 40). Whether

such a comprehensive examination of compliance with EU law exists, the Advocate General considered that it is for the domestic court to determine (para 41). However, the Advocate General rejected that the procedure for infringement of EU law against the Member States can substitute the comprehensive assessment of the award approach. The reason behind this being that the infringement proceedings are 'cumbersome' and cannot guarantee the effectiveness of EU law (para 60).

Individual arbitration agreements between a Member State and an investor are to be distinguished from commercial arbitration agreements

The Advocate General noted that the CJEU case-law accepts commercial arbitration between private parties, despite being subject to a limited review for compliance with EU law (paras 43-46). As provided for in the *Achmea* judgement, the Advocate General stated that such a commercial arbitration is permissible as it is the expression of the free will of the parties (para 47). However, the Advocate General rejected that the investor and the State in the case concerned are on equal footing. Rather, the case concerns the exercise of sovereign powers of the State on the investor by subjecting it to banking supervision (para 54). Thus, for the Advocate General there can be no question of free will on the part of the investor, nor it is likely that a State will subsequently conclude an arbitration agreement concerning its sovereign measure of its own free will (para 54).

Above all, the Advocate General considered that the commercial arbitration exception between private parties is not applicable to the arbitration agreement between an investor and a Member State by virtue of Article 344 TFEU (paras 55-58). This Article, which does not apply to private parties, precludes Member States from removing disputes relating to EU law from the application of the EU judicial system (para 58).

Individual arbitration agreements and the principle of equal treatment

The Advocate General noted that the individual arbitration agreement must be in accordance with the principle of equal treatment (para 71). This principle requires similar situations to not be treated differently without justification (para 67). For the Advocate General the right only some investors to have recourse to arbitration, whereas others could only have recourse to national courts, constitutes unequal treatment (para 68). While the Advocate General considered that it is 'difficult to conceive' a justification for this unequal treatment, it held that it is for the domestic court to determine whether such a justification is present (para 70).

The form of the arbitration agreement

The Advocate General considered that the form of the arbitration agreement is irrelevant for the compatibility with the EU law (paras 72 and 78).

No limited temporal effect for the *Achmea* judgment

PL Holdings has requested CJEU to apply the *Achmea* judgement only to future arbitrations. However, the Advocate General recommended against such temporal limitation, as 'the unrestricted permissibility of arbitration agreements on the basis of late objections regarding the competence of the arbitration tribunal would temporarily deprive that judgment of its practical effect' (para 84).

Conclusion

Should the CJEU follow the Advocate General's Opinion it is a welcome clarification that on the condition that the award can be subject to comprehensive judicial review, arbitration agreements are not per se incompatible with EU law.