Lex Scientia Law Review

Volume 6 Number 1 June, 2022

Type: **Research Article**

Digital Globalization and Law

Stefan Koos✉

Universitaet der Bundeswehr Munich, Germany

✉ Corresponding email: stefan.koos@unibw.de

Abstract *The regulation of social processes is part of a state's sovereignty. States apply their law to shape and control social and economic conditions within their territory. Law as an instrument for coordinating human behaviour and for balancing colliding interests within the society is linked to human behaviour, either individually or within human organisations. The basic prerequisite for the existence of law is human interaction based on emotions, desires, and the pursuit of interests. Law and trust (interpersonal trust or system trust) are connected to each other. This leads to the assumption that law loses its relevance with a decrease of the relevance of trust. This article explores the question of which factors of current and future digitalisation could lead to a loss of the relevance of trust and of the relevance of the aspect of human behaviour as a connecting factor for legal norms. The article concludes that technological globalisation and ubiquity of the internet have already led to a loss of state territorial sovereignty. This has resulted in the diminution of system trust in law. The article further shows how digitalisation is pushing back the relevance of human behaviour and emotionality and, therefore, technicity is increasingly displacing law. The article describes the connection between deterritorialization and the development of new disruptive digital technologies and asks about the future role of ethics in the legal system of an advanced digitalised society. The development of concrete solutions and legislative proposals is subject to further studies.*

Keywords Digitalization, Territorial Principle, Legal Ethics, Artificial Intelligence

1. Introduction

New digital technologies, which are still at the beginning of their development, such as blockchain technology, virtual reality, augmented reality, or artificial intelligence, have the potential to change the society radically, even more than the internet did. This article is about disruption and a rather pessimistic view of the role of law in the future. It deals with the concept of disruption because, for the first time since the emergence of the major continental European civil law codifications, real disruptions in the law are to be expected, which may not only lead to a need for adjustments and additions to civil law figures, but which may also affect the methodology of law application and enforcement. Moreover, it is also to be expected that outdated rules of international law and conflict of laws based on the principle of territoriality will no longer lead to adequate results and that the formation of alternative technical extra-legal regulatory and control structures will be promoted. The article is pessimistic because precisely this shift of control and governance from law to extra-legal structures and technical instruments will create a problem for the state's mandate to protect its citizens, whose regulatory leeway is dwindling. If the shift from legislative regulation to technology continues, the legislature will only be in a very limited position to adequately enforce principles of justice or humanistic and social purposes of the law. This may also imply a problem for the constitutional mandate of the state.

The article identifies various aspects of the technologization of the society and shows that, as digitisation continues to develop, even stronger disruptive factors could emerge than before. These can lead to strongly changed framework conditions for law, which could also cause a re-evaluation of a basic concept of private law. For example, the concept of human 'conduct', which is essential for private law and which, within the framework of the legal principle of private

autonomy, is linked to a constitutionally protected freedom concept,[1] might no longer fit. Law as a social instrument for behavioural steering, conflict solution and limitation, shaping of living conditions and social organisation is based on the idea of human unpredictability and the coordination of individual and collective interests of the individuals of a society and, in general, the balancing of interests of all members of society. Thus, the basic prerequisite for the existence of law is human interaction based on emotions, desires, and the pursuit of interests. Law is closely related with trust, whether the law replaces, reinforces, or establishes trust among actors. Law and trust are therefore linked, which leads to the assumption that law loses its meaning without trust. The main thesis of this study is: *trust in law is losing relevance and is increasingly being replaced by technical determinacy.*

The study not only aims to contribute to the law of digital technologies, but rather to continue earlier studies of the author on conflict of laws and globalisation. The author has described before the loss of importance of the territoriality principle, based on state sovereignty, for the conflict of laws in competition law and intellectual property law as a result of the economic globalization and of a deterritorialization effect of the internet.[2] This article aims to consistently continue this approach in relation to 'digital globalisation' by raising the question of whether states are entitled to enforce extraterritorially certain interests in the application of their national law in a ubiquitous digital society using their economic and political power to protect its citizens as a reaction to a loss of territorial sovereignty. In this way, it transfers the idea of the loss of significance

[1] Stefan Koos, 'Machine Acting and Contract Law – The Disruptive Factor of Artificial Intelligence for the Freedom Concept of the Private Law', UIR Law Review 5, no. 1 (2021): 1–18.

[2] Karl-Heinz Fezer and Stefan Koos, *Internationales Wirtschaftsrecht*, 5th ed., Staudinger BGB (München: Sellier/de Gruyter, 2019), paragraph 11 and 950.

of territoriality previously developed for economic globalisation to the progressive process of a *technologically based digital globalisation*.

Furthermore, this study aims to set other recent articles by the author on the impact of digital technologies on private law, economic law, and data protection law[3] in a broader frame of reference. Technologies such as artificial intelligence,[4] augmented and virtual reality as well as blockchain and tokenisation[5] have the potential for a real disruptive effect on law. It will be discussed which consequences this may have for the role of the law in the future. The relationship between law and technology has already been addressed previously: particularly *Lessig*'s study of the relationship between the 'East Coast Code' and the 'West Coast Code' must be mentioned.[6]

---

[3] Stefan Koos, 'Protection of Behavioural Generated Personal Data of Consumers' (1st Workshop on Multimedia Education, Learning, Assessment and its Implementation in Game and Gamification in conjunction with COMDEV 2018, Medan Indonesia, 26th January 2019, WOMELA-GG, Medan: EAI, 2019), http://dx.doi.org/10.4108/eai.26-1-2019.2283267; Stefan Koos, 'Digitalization of University Education and Research as Consequence of the Covid-19 Pandemic - A Paradigmatical Change' (1st Multidisciplinary International Conference on Potential for Research During the Pandemic, Surabaya 15.-16. December 2021, submitted, 2021).

[4] Stefan Koos, 'ARTIFICIAL INTELLIGENCE – SCIENCE FICTION AND LEGAL REALITY', *Malaysian Journal of Syariah and Law* 6, no. 3 (20 December 2018): 23–29; Stefan Koos, 'Artifical Intelligence as Disruption Factor in the Civil Law: Impact of the Use of Artifical Intelligence in Liability, Contracting, Competition Law and Consumer Protection with Particular Reference to the German and Indonesian Legal Situation', *Yuridika* 36, no. 1 (2021): 235–62; Koos, 'Machine Acting and Contract Law – The Disruptive Factor of Artificial Intelligence for the Freedom Concept of the Private Law'.

[5] Stefan Koos, 'The Individual and the Property in Virtual Worlds' (submitted, 2022).

[6] Lawrence Lessig, *Code and Other Laws of Cyberspace* (New York: Basic Books, 2000), https://lessig.org/images/resources/1999-Code.pdf; see also from Germany on the relativisation of law through digitalisation Volker Boehme-Neßler, 'Die Macht der Algorithmen und die Ohnmacht des Rechts. Wie die Digitalisierung das Recht relativiert', *Neue Juristische Wochenschrift* 70, no. 42 (2017): 3031–37.

2. Method

The study is based on a normative legal approach using international literature, judicative research, and analysis of legislation. It includes law comparison. It is an evaluative analysis of the impact of the digitalization on contemporary and future private law. The study is based on a pluralistic approach to law, integrating social, economic and ethic aspects.

3. Result & Discussion

1. Deterritorialization through Digital Ubiquity

Already the development of the internet was partly perceived as disruptive. This was certainly true for the field of economics. However, for the private law, it must be strongly doubted that a 'disruption' had already arisen with this. For law, a disruption only occurs when the technical innovation leads to the existing legal principles systematically underlying the legal system no longer being applicable. Accordingly, the uprise of the internet was not a real disruption in civil law.[7] Indeed, it turned out that the internet did not change the existing civil law institutes and instruments. These were still sufficient to cover and solve all occurring legal situations. Regarding contract law, for example, the internet has only changed the medium and speed of legally relevant communication processes. However, digitalisation through the internet has initiated a process that leads to a loss of state territorial authority, because numerous processes of social and economic life take place on a ubiquitous level and can no longer be clearly assigned to state territories. So even if the internet did not mean a disruption for the

[7] Koos, 'Machine Acting and Contract Law – The Disruptive Factor of Artificial Intelligence for the Freedom Concept of the Private Law', 2; Koos, 'Artifical Intelligence as Disruption Factor in the Civil Law'.

concepts of private law, since the basic legal institutions remained applicable, it did lead to distortions with regard to the foundations of the international law and especially the conflict of laws, because the enforceability of state law is in part reduced. On the other hand, international law has suffered a considerable loss of importance because it is based on the very idea of territorial sovereignty and the principle of territoriality, which is contradicted by the ubiquity[8] of the internet.[9]

At the same time, there has been a shift from the purely territorial legal control of certain facts to the limitation or the expansion of power of states and economic blocs, depending on their economic or political strength. Certain states or blocs can extend their economic law extraterritorially. The extraterritorial application of national economic law *per se*, especially of antitrust law, is not a new phenomenon. It has been strongly discussed in the German antitrust law literature since the 1980s and criteria for limitation have been developed, derived in particular from international law.[10] Based on the doctrine of a 'reasonable

---

[8] The concept of the *ubiquity principle* in the German conflict of laws is initially understood as the rule that the injured party in a cross-border tort can decide whether to invoke the law of the place where the event which gave rise to the harm occurred (*'Handlungsort'*) or the place where the harm arose (*'Erfolgsort'*), see Fezer and Koos, *Internationales Wirtschaftsrecht*, paragraph 397 and 1137; Christopher L. Blakesley and Otto Lagodny, 'Finding Harmony Amidst Disagreement Over Extradition, Jurisdiction, The Role of Human Rights, and Issues of Extraterritoriality Under International Criminal Law', *Vanderbilt Journal of Transnational Law* 24, no. 1 (1991): 15; in the European Union and German international competition law, this principle is superseded by the effects doctrine (*'Auswirkungsprinzip'*) or the market place principle (*'Marktortprinzip'*). The ubiquity principle is to be distinguished from the assumption of unlimited worldwide applicability of German law by the former German *Reichsgericht* (universality principle, *'Universalitätsprinzip'*), see Fezer and Koos, 444. In German international criminal law, this last-mentioned principle is found in Sec. 9 para.1 of the Criminal Code (StGB).

[9] Fezer and Koos, *Internationales Wirtschaftsrecht*, paragraph 12.

[10] Hannah L. Buxbaum, 'Territory, Territoriality, and the Resolution of Jurisdictional Conflict', *American Journal of Comparative Law* 57 (2009): 653.

connection' ('*sinnvolle Anknüpfung*'),[11] the *effects doctrine* in antitrust law's conflict of laws[12] is considered to be in principle in conformity with international law,[13] if there is a regulatory interest of the state that is worthy of protection and if the chosen criterion of connection is appropriate. Limitation criteria of an international law nature were based on the principle of *comitas gentium* and the principle of non-interference. From this, limitation criteria such as a duty to weigh the state's own interests in applying the law against the interests of other states or the limitation to direct or foreseeable effects were derived in order to implement a self-restriction of the effect of national antitrust law to its own territory.[14] One consequence of the endeavour to limit the extraterritorial effect of the domestic economic law was the earlier case law of the European Court of Justice not to explicitly apply the antitrust conflict-of-law effects doctrine,[15] but to base the applicability of European antitrust law on an 'implementation of the cartel in the

[11] Rolf Bär, *Kartellrecht Und Internationales Kartellrecht* (Bern: Stämpfli, 1965), 101.

[12] The effects doctrine states that a state's own national antitrust law shall apply to a cross-border antitrust case if the conduct restricting competition actually or potentially affects the market of that state, see Art. 6 par. 3a European Commission, 'Regulation (EC) No. 864/2007 of the European Parliament and of the Council of 11 July 2007 on the Law Applicable to Non-Contractual Obligations (Rome II)' (2021); Federal Republic of Germany, 'Act against Restraints of Competition (GWB)' (n.d.); on the German effects doctrine compared to the US-Law see Buxbaum, 'Territory, Territoriality, and the Resolution of Jurisdictional Conflict', 640–42.

[13] Karl Matthias Meessen, *Völkerrechtliche Grundsätze des internationalen Kartellrechts* (Baden-Baden: Nomos, 1975), 158.

[14] See for the discussion of the criteria based on international law principles Fezer and Koos, *Internationales Wirtschaftsrecht*, paragraph 149.

[15] Bernadette Zelger, 'EU Competition Law and Extraterritorial Jurisdiction – a Critical Analysis of the ECJ's Judgement in Intel', *European Competition Journal* 16, no. 2–3 (2020): 618.

common market'.[16] Even though the result of the application of this criterion corresponded to the effects doctrine, the ECJ has only recently also explicitly referred to the effects doctrine.[17] This restraint on the part of the Court is likely to have been based on consideration for a principle of territoriality founded in the *comitas gentium* principle of the international law.[18]

With the increasing worldwide interconnection of markets in the context of the economic globalisation,[19] but above all with the reduction of the importance of territorial borders in the internet era, the principle of territoriality is becoming less important,[20] because a territorial allocation and limitation of market effects are no longer possible in many cases.[21] Thus, the problem of the extraterritoriality of national law and its legitimacy and limitation gains a new, stronger significance:

Firstly: State sovereignty is overlaid by the facticity of the virtual space. Insofar as facts take place virtually, they can indeed affect the territory of a certain state, but national law has only limited options to deal with this interference, insofar as the causer is not on the territory of the state or the technical cause cannot

[16] A. Ahlström Osakeyhtiö and others v Commission of the European Communities ('Wood Pulp'), No. 89/85 (European Court of Justice 27 September 1988); see Buxbaum, 'Territory, Territoriality, and the Resolution of Jurisdictional Conflict', 642.

[17] Intel Corp. v European Commission ('Intel'), No. C-413/14P (European Court of Justice 6 September 2017).

[18] Stefan Koos, 'Globalisierung, Extraterritorialität und internationalisierte sozial verantwortete Interessenverfolgung im Wettbewerbsrecht', in *Marktkommunikation Zwischen Geistigem Eigentum und Verbraucherschutz: Festschrift für Karl-Heinz Fezer zum 70. Geburtstag* (München: C.H.Beck, 2016), 265.

[19] Fezer and Koos, *Internationales Wirtschaftsrecht*, paragraph 142.

[20] Stefan Koos, 'Global Responsibility and International Mutual Consideration in the Business Law - Theory and Reality', in *Proceedings 6th AFHI Conference* (6th Conference of the Indonesian Asociation for Legal Philosophy (AFHI) - 'Antinomi Hukum - Pluralisme ataukah Integrasi' Bandung 17.-18. November 2016, Bandung: Epistema Institute, 2016), 21–28.

[21] Koos, 'Globalisierung, Extraterritorialität und internationalisierte sozial verantwortete Interessenverfolgung im Wettbewerbsrecht', 270.

be located and eliminated in the respective state territory. Insofar as state courts decide against such interferences, their judgements can in principle only relate to their own national territory. However, since infringement is ubiquitous on the Internet and cannot be territorially delimited, an injunction would possibly be territorially overbroad and would have extraterritorial effect.[22] At the very least, national law cannot be effectively enforced because there is no executive power of a state outside its own territory.[23] The same applies, for example, to data protection issues on the internet.

Secondly: Some states can extend the effects of their national legal norms beyond their own national territory and enforce them extraterritorially. However, this is not based on a general legitimacy of extraterritorial application of law, but on the *de facto* consideration of global companies for the law of these states and on the interest of companies to behave in a legally compliant manner in markets which are important for their global business activities. Politically and economically weaker states, on the other hand, have little chance of enforcing their national law at the international level. This is an example of how law loses importance in a technical globalisation because the conflict-of-law principle, which has been widely respected up to now, gives way to a principle of 'enforcement of the strongest'. The principle of law is thus displaced by a political principle. Politically, this aspect of the 'law of the strongest' may be justified with the viewpoint of a 'self-defence' of the sovereign state against the otherwise uncontrollable influence from outside through globally digitalised platforms. The breaking of the principle of avoiding extraterritorial overregulation could be understood as a direct political reaction to the decline of state sovereignty.

---

[22] See the case Playboy Enterprises Inc. v Chuckeberry Publishing Inc., No. 939 F.Supp. 1032, 1040 (US District Court for the Southern District of New York 19 June 1996).

[23] Fezer and Koos, *Internationales Wirtschaftsrecht*, paragraph 1153.

This is clearly illustrated by the example of the data protection law of the European Union: The European General Data Protection Regulation (GDPR)[24] contains a provision on its extraterritorial applicability in Article 3 (2): Regardless of the registered office of the processor or the place of processing, the connecting factor for the territorial scope of application of the GDPR is the fact that it concerns personal data of persons in the European Union. Due to this connecting factor, the GDPR has a significant impact beyond the territory of the EU. This extraterritorial impact is particularly explosive because it is not actually based on legislative legitimacy to regulate data protection worldwide, but on the economic importance of the EU's internal market: market-powerful companies based outside the EU will observe the EU data protection rules simply because the European internal market is of great relevance to them.[25]

As a result, it is possible that a legitimacy of extraterritorial enforcement of the own law by a market-powerful state or confederation of states can be explained as the flip side of the loss of territorial law enforcement power as a result of the

[24] European Union, 'Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)' (2016).

[25] This can currently be seen in the conflict between the US company Meta and the European Union: Meta has threatened to block the Instagram and Facebook platforms for users in the EU in view of the strict prohibition of the EU Data Protection Regulation on the transfer of personal data of EU citizens to the USA and the lack of a safe harbour agreement on data transfer between the EU and the USA. The reactions of German and French government officials to this were rather relaxed. Meta then denied the announcement: Jillian Deutsch and Stephanie Bodoni, 'Meta Renews Warning to E.U. It Will Be Forced to Pull Facebook', *Time*, 8 February 2022; In fact, it seems unlikely that Meta will forgo the EU market, given advertising revenues of $6.8 billion annually in the EU, Vishal Mathur, 'Call the Bluff: Meta Cannot and Will Not Unfriend Europe', *Hindustan Times*, 8 February 2022. However, the conflict shows that EU data protection rules are also respected in principle by US companies with strong market power.

ubiquity of the internet: The protection of the own citizens on the own territory against encroachments on their personal rights interests from outside - for example, by foreign information technology or global technology companies - is greatly impeded due to the lack of territoriality of virtual space. Since the territoriality of information on the Internet is not, or only imperfectly, given, a state ban on corresponding activities conversely necessarily has an extraterritorial reach, insofar as the activity cannot be effectively refrained from exclusively on the territory of the state in question. Decisions by national courts to ban internet information then necessarily have an effect that extends beyond the state's own territory.

The example of augmented reality glasses, which are permanently connected to the internet and generate not only movement data of their wearers, but also data of unsuspecting persons who are scanned with the glasses, illustrates how future information technology eliminates the data protection law concept of the individual's control over his or her data. If smart glasses are increasingly used in public, this can lead to everyone who moves in public potentially becoming a target of private surveillance without being able to consent to it or escape it. This can lead to a change in the behaviour of individuals in society if everyone is always aware that they can become the target of observation and profiling (for example, with facial recognition) at any time.[26]

[26] It is instructive to note that in 1983, in the so-called 'census judgement' ('Volkszählungsurteil'), the German Federal Constitutional Court referred to the effects of surveillance on citizens' behaviour and individual self-determination (*translation by the author*): "*Anyone who is not able to assess with sufficient certainty which information concerning him or her is known in certain areas of his or her social environment, and who is not able to assess to some extent the knowledge of possible communication partners, can be significantly inhibited in his or her freedom to plan or decide on the basis of his or her own self-determination. The right to informational self-determination would not be compatible with a social order and a legal order enabling it in which citizens can no longer know who knows what, when and on what occasion about them. Those who are uncertain whether deviant*

Furthermore, the loss of state control over matters relevant to data protection law becomes obvious here because an outflow of data to other states with a lower level of data protection or an ideologically justified interest in the global control of individuals could in fact only be completely prevented by a legal ban on corresponding products. However, such a ban is neither economically desirable nor would it be possible to enforce it in the long term. The legitimate interest of states to protect the data protection interests of their citizens, which is also recognised under international law, can therefore hardly be satisfied. It therefore seems legitimate for states - in a kind of 'self-defence reaction' - to try to enforce the need for protection of their citizens and their economic area at least through an existing de facto market power. *The principle of ubiquity thus displaces the principle of territoriality as a principle of order based on international law principles*, and one could say that a principle of power of the economically strong blocs - the 'right of the strongest' - takes its place.

If a state seeks to avoid the loss of control described above, especially if a state is unable to enforce respect for its legal norms extraterritorially, the alternative would be a pragmatic restructuring of the law. In data protection law, this could be done by the legislator focusing on strengthening an immaterial data ownership of personal data[27] and the personal responsibility of citizens in disclosing their personal data instead of prohibitive approaches to the protection of personal

behaviour will be noted at any time and permanently stored, used or passed on as information will try not to attract attention through such behaviour.", 'Volkszählungsurteil', 1 BvR 209/83, BVerfGE 65, 1-71 (Bundesverfassungsgericht, Urteil des Ersten Senats 1983). It is possible that the transformation to a digital information society that has taken place in the meantime has already strongly reduced citizens' sensitivity compared to the situation in the year 1983. The consequence of this would be that a greater intensity of personality visibility in public may be tolerable, at least with regard to the aspect of influence on individual self-determination.

[27] See to the intellectual property approach Karl-Heinz Fezer, *Repräsentatives Dateneigentum - Ein zivilgesellschaftliches Bürgerrecht*, Studie der Konrad-Adenauer-Stiftung e.V., 2018.

data.[28] However, this would be associated with a paradigm shift in data protection law, in that citizens would no longer be allowed to rely on state prohibitions of actions that violate the law, and the state would legally permit far more data protection-relevant interventions than before. On the one hand, this could be justified by the fact that society's understanding of its need for protection in the digitally globalised world has changed in comparison to the pre-digital era in all areas of social life. On the other hand, however, this also means a certain 'capitulation' of the law to technological facticity, especially since international law in its current form does not seem to be suitable for replacing the no longer sufficient national regulations with genuine global regulatory approaches.

The loss of state sovereignty because of the ubiquity of the internet and the factual replacement of the principle of territoriality by the principle of ubiquity also becomes clear in intellectual property rights. Here, a 'crisis of conflict of laws' is particularly evident because of the digital globalisation. The scope of national intellectual property rights is historically linked to the reach of state sovereignty and thus limited to the national territory.[29] This follows from the principle of national limitation of the sovereign act of granting.[30] From this, the Country of

[28] Koos, 'Machine Acting and Contract Law – The Disruptive Factor of Artificial Intelligence for the Freedom Concept of the Private Law', 10–11.

[29] Lydia Lundstedt, *Territoriality in Intellectual Property Law* (Stockholm: Stockholm University, 2016), 28.

[30] The Territoriality principle is recognized by international customary law. It results also from the principle of National Treatment in several international treaties such as the TRIPS or the Paris Convention for the Protection of Industrial Property. See also Grupo Gigante v Dallo&Co., No. No 00-57118 (US Court of Appeals for the Ninth Circuit 15 December 2004); See for the Japanese court practice Teruo Doi, 'The Territoriality Principle of Patent Protection and Conflict of Laws: A Review of Japanese Court Decisions', *Fordham International Law Journal* 26, no. 2 (2002).

Protection principle (*lex loci protectionis*)[31] is usually derived for conflict of laws.[32] On the one hand, the principle of territoriality is based on the territorial limitation of the state's power to enforce the law. On the other hand, it is an expression of the respect of national legal systems for sovereignty of other states. Thus, the principle of territoriality, like the effects doctrine, is related to the international public law principle of *comitas gentium*, which, as shown above, is also a justification for the discussed limitations of the extraterritorial effect of the effects doctrine under conflict of laws.

In the era before the development of the internet, the localisation of domestic IP-law infringements was regularly unproblematic. Works protected by copyright, for example, were only available in analogue or embodied digital form. Trademark infringements regularly occurred using the trademark on products or in print media. On the internet, infringements regularly take place completely independently of national territories. In principle, the interests of the right holder are potentially affected wherever the relevant information can be retrieved from the internet. The question thus arises as to the effects of the ubiquity of the internet on international economic law based on the territorial sovereignty of states and especially on national conflict of laws.

---

[31] The Country of Protection principle states that the law of the country for whose territory protection is sought/claimed is applicable with regard to infringements of property rights. Because of the territoriality the national law is basically only dealing with infringements of intellectual property rights on its own territory. However, the *definition of an domestic infringement* (localisation of the infringement, 'Eingriffslokalisierung') by the IP-law of this state can be more or less excessive and may sometimes lead to an extraterritorial effect, see Fezer and Koos, *Internationales Wirtschaftsrecht*, paragraph 937-938 and Peukert, 'Territoriality and Extraterritoriality in Intellectual Property Law', 13–14. In the European Rome II Regulation (Regulation No 864/2007 on the applicable law to non-contractual obligations), the Country of Protection principle is found in Art 8(1).

[32] Peukert, 'Territoriality and Extraterritoriality in Intellectual Property Law', 6–7.

This results in a difficult methodological problem because the territoriality principle requires that the facts of the domestic act of infringement are not excessively expanded. So, criteria for an appropriate limitation of the applicability of national IP-law to cross-border matters must be applied. Such criteria of a sufficient domestic relationship of the matter are difficult to define, they can be of a quantitative or qualitative nature. Ultimately, however, it becomes apparent that the territorial concept of IP-law can only with difficulty be brought into line with the cross-border nature of the internet.

As in the example of data protection law, it is also clear here that national law can sometimes no longer counter violations on the internet sufficiently effectively. Even if a violation of domestic law can be found, the prohibitive competence of a national court is limited to its own territory. However, internet violations cannot be limited territorially. A national judge can therefore basically not order the deletion of a certain information on the internet concerning an infringement by the worldwide web without exceeding his territorial competence. If this nevertheless happens, these are examples of extraterritorial effects of national law, which only have a chance of being effectively enforced if the infringer complies with the order, for example, out of consideration for the importance of a national market. For the legitimation of these extraterritorial effects and their enforcement by virtue of power, the 'self-defence' considerations outlined above then apply.

2. The Loss of Importance of Law in the Digitalization

In a society increasingly characterised by ubiquitous global communication structures, the principle of territoriality is no longer a fully suitable legal principle. This raises the question of the relevance of law in the progressively digitalised society. If the options for enforcing state interests in the application of the own domestic law dwindle, then this is a sign of the loss of significance of law in

general. This can lead to an increasing loss of trust in the state's ability to protect the interests of its citizens. Based on his view of the function of law, the German sociologist *Luhmann* stated that law which is not respected or not sufficiently enforced requires the system to resort to more immediate forms of securing trust.[33] From this point of view, it is not surprising if *technical instrumentalities of control and security*, independent of territoriality, are developed and become more important with the degree of technical deterritorialization, e.g., safety-by-design or blockchain solutions. In a rather pessimistic view of the future of law in a 'digital society 5.0', *Shidarta* 2021 emphasised the increasing importance of legal ethics at the *2nd International Conference on Law, Economy and Governance* at Universitas Diponegoro in Semarang.[34] According to his presentation, there is a shift from regulation by virtue of state sovereignty to monitoring and self-regulation by technology corporations. To prevent this, the law must develop regulatory approaches before corresponding technical innovations which further restrict sovereignty become established in society. In this respect, there is a race between law and technological change.

In the example of augmented reality glasses, too, the race between the development of appropriate regulatory structures and the social penetration of a new technology that poses a severe threat to the legal interests to be protected seems almost lost. The conclusion to be drawn from this is pessimistic, even resigned: the individual may no longer trust the protection by state law in any case, since due to ubiquity, state sovereignty, at least of weaker states, is no longer sufficient to effectively protect the legal interests of the citizens against violations

[33] Luhmann, *Das Recht der Gesellschaft*, 132.

[34] Shidarta, 'Ethics and Law in a Digital Society - A Study of Legal Philosophy' (2nd International Conference on Law, Economic and Governance ICOLEG 2021, Universitas Diponegoro, 29 June 2021), https://youtu.be/Fnp90LxtVe8.

and exploitation by big technology corporations or by foreign states. The loss of trust could lead to greater indifference on the part of the citizens. In data protection matters for example this could lead to the paradox effect that individuals even more willingly make their private data available to powerful platform companies than necessary.

3. The Replacement of Trust by Technicity

Reduced state sovereignty and reduced options for effective national law enforcement could be compensated for by technical innovations in the globally digitalised society. Developments in the field of artificial intelligence, smart contracts and the blockchain technology could offer instruments in the future that enable the protection of interests independent of state sovereignty.

A central aspect in this context is the replacement of emotionality by determined rationality. Negotiation situations are characterised by trust and mistrust as opposites. Contracts are the result of negotiations or an abstract interest equilibrating process (e.g., standard clauses following from anticipated negotiation situations). They express a certain interest balance. The contract is ultimately a result of mistrust between the parties. The contractually regulated aspects of the facts lead to trust of the parties in the authoritativeness of the outcome of the negotiations. The contracting parties trust to a certain extent that the contract will be fulfilled. The law of irregularity in performance, which regulates the legal consequences of non-compliance by a counterparty, is in turn an expression of mistrust in the reliability of the parties. The same applies to the procedural possibilities of enforcing claims. Trust also plays an important role here because the parties trust the court to enforce the law. This concerns the system

trust,[35] here the trust in the functioning of the legal system as opposed to interpersonal trust[36] in the negotiating partner. In parallel societies where state law enforcement does not enjoy sufficient acceptance, self-organised alternative dispute resolution mechanisms occasionally take the place of state procedures.

It is not the intention of this article to discuss the different ideas in jurisprudence, economics, and sociology on the relationship between 'trust' and 'law'. For example, it is said that trust replaces law,[37] or that trust is only needed where law does not offer sufficient sanctions and enforcement options. Conversely, it is also said that law replaces trust or makes it obsolete,[38] or that law establishes trust.[39] It is possible that a clear definition of the relationship between trust and law is not possible[40] due to the lack of a clear definition of 'trust'.[41] The first thing to establish here is that there is an antinomy between emotionality as a

---

[35] For Luhmann, *Vertrauen: Ein Mechanismus der Reduktion sozialer Komplexität*, 28, Trust (*'Vertrauen'*) is firstly personal serving as an instrument to bridge uncertainty in the behaviour of other persons. With the growth of a need for complexity it changes to system trust (*'Systemvertrauen'*). This system trust is connected with a *`consciously risked renunciation of possible further information, as well as proven indifferences and ongoing success control`* (translation from German by the author).

[36] Definition of interpersonal trust at Randy Borum, *The Science of Interpersonal Trust*, Mental Health Law & Policy Faculty Publications 574 (University of South Florida, 2010), 2; on the term trust Jeffry A. Simpson, 'Chapter 25: Foundations of Interpersonal Trust', in *Kruglanski/Higgins (Ed.) Social Psychology - Handbook of Basic Principles*, 2nd ed. (New York/London: The Guilford Press, 2007), 588.

[37] Friedrich Darmstädter, 'Recht und Jurist', *Süddeutsche Juristen-Zeitung* 3, no. 8 (1948): 433–34.

[38] Katharina Beckemper, 'Das Rechtsgut "Vertrauen in die Funktionsfähigkeit der Märkte"', *Zeitschrift für Internationale Strafrechtsdogmatik (ZIS)*, 2011, 320.

[39] Paul J. Zak and Stephen Knack, 'Trust and Growth', *The Economic Journal*, 2001, 316.

[40] Susan P. Shapiro, 'The Social Control of Impersonal Trust', *American Journal of Sociology* 93, no. 3 (1987): 625.

[41] Dieter Schmidchen, *Vertrauen und Recht: Eine ökonomische Analyse*, CSLE Discussion Paper 2000–04 (Saarbrücken: Universität des Saarlandes, Center for the Study of Law and Economics (CSLE), 2000).

factor of uncertainty on the one hand and the determinacy of technical processes on the other. Trust, whether interpersonal or system-related, is related to emotion. Uncertainties exist in human relationships and social processes that are based on human behaviour. Such uncertainties require trust, even to the extent that the probability of certain human decisions in the future is increased by contractual ties or legal enforcement options. *Luhmann* stated that law has the function of stabilising "*normative expectations by regulating their temporal, factual and social generalisation*".[42] He wrote:

> *"The Law makes it possible to know with which expectations one will find social support, and with which one will not. If there is this certainty of expectations, one can face the disappointments of daily life with greater serenity; one can at least rely on not being discredited in one's expectations."*[43]

Law is a mechanism that reduces the complexity of social interactions by providing the basis for trust in regulated social processes.[44] Law which is not respected or effectively enforced leads to the need for alternative, more immediate forms of trust assurance.[45] One such immediate form of trust assurance could be seen in technicity: There are indications of the displacement of certain elements of

---

[42] Luhmann, *Das Recht der Gesellschaft*, 131. Translation from German by the author. German original: *"…normative Erwartungen durch Regulierung ihrer zeitlichen, sachlichen und sozialen Generalisierung…".*

[43] Luhmann, 132, translation from German by the author. German original: "*Das Recht ermöglicht es, wissen zu können, mit welchen Erwartungen man sozialen Rückhalt findet, und mit welchen nicht. Gibt es diese Erwartungssicherheit, kann man mit größerer Gelassenheit den Enttäuschungen des täglichen Lebens entgegensehen; man kann sich zumindest darauf verlassen, in seinen Erwartungen nicht diskreditiert zu werden.*".

[44] Luhmann, *Vertrauen: Ein Mechanismus der Reduktion sozialer Komplexität*, 40–41.

[45] Luhmann, *Das Recht der Gesellschaft*, 132.

social control, which are only effective to a limited extent, by technical instruments that secure certain processes and legal positions in a determinate manner without depending on law enforcement and control by human action. Such a process would not only be a functional displacement of law by the factual, but also a 'capitulation of trust' and thus a 'de-humanisation'. It is true that there is also a kind of system trust in this respect - namely in the functioning of technical safeguards. Blockchain technology, as a "[t]rusted and efficient way of sharing data and transactions",[46] generates trust through unchangeable and openly visible entries. The relationship of the trust generated in the blockchain to the trust existing in a fiduciary trust structure, for example, is characterised by the immutability of the entry and thus, in contrast to the interposition of neutral trustees in a bilateral relationship between two parties, is technically conditioned. This system trust, however, refers to determined processes of technology or technical safeguards and not to human action or organisational structures.

The phenomenon of technicity changing, or displacing law can be found exemplarily in the following six aspects:

1. The replacement of human decision-making processes by decisions of artificial intelligence systems leads to a *replacement of emotionality by determinacy*. The decision of the AI system itself is determined. From a human point of view, decisions by AI systems can indeed be erroneous. However, law cannot counter such errors at the level of the decision-making process: they cannot be normatively evaluated because artificial intelligence, as a determined system, has no freedom of decision. If one wants to legally grasp the harmful result of machine action, one can only do so at the level of the programming or training of the system. Law will therefore - for the time being - not be completely displaced. Rather, liability issues

[46] Anthony Welfare, *Commercializing Blockchain - Strategic Applications in the Real World* (Hoboken, 2019), 7.

and evaluations will continue to arise at the level of product development and programming. A further stage in the displacement of law will be reached when programming is no longer done directly by humans, but artificial intelligence itself generates new artificial intelligence.

2. We see a shift of decision-making processes relevant to fundamental rights from human decision-makers to artificial intelligence systems. One example is the use of AI-controlled upload filters as part of platforms' copyright compliance measures and, comparably, the use of corresponding filters to detect and delete hate speech or false information on internet platforms and social media. These developments are also a consequence of - in principle justified - legislative requirements for platforms and social media. The introduction of AI upload filters follows indirectly for copyright from Art. 17(4) of Directive (EU) 2019/790 on Copyright and Related Rights of 17.4.2019 (Digital Single Market Directive). Liability of platform operators is already provided for if they have not taken sufficient measures to prevent the upload of copyright-infringing content, which in fact forces platforms to carry out an algorithm-driven analysis and filtering of uploaded content. The fact that the regulation leads to non-human-controlled content filtering by AI is made clear by Art. 17 (9) sentence 3 DSM-D, which explicitly provides for a review of a blocking of access to relevant information or its removal by humans. As such, filtering by algorithms represents a restriction of freedom of expression and other legal positions such as artistic freedom, because it is accepted that the algorithm could also block legally permissible content in individual cases due to faulty analysis. This becomes even clearer with the use of algorithm-based filters, which filter the publication of statements in social media for fake news or hate speech, partly still based on mere keyword analysis. The tendency to transfer evaluative decisions which are flexible and dependent on semantic aspects to algorithms can also be seen as consequence of the loss of

control of the law: Control functions relevant to fundamental rights are delegated from the state to the platform companies, as classical legal control capitulates to the speed and ubiquity of the internet. On the other hand, it is also a symptom of the phenomenon of the 'law of the strongest', because platforms are forced to prevent uploading for the platform as a whole and will only implement corresponding measures - albeit then with global consequences - if the relevance of the law-making state's market is big enough. Furthermore, this is also an example of the loss of trust in the human controllability of facts on the internet. This leads to the replacement of legal prevention directed at human behaviour with control by means of technology.

3. Smart contracts, computer protocols designed to digitally facilitate, control, or enforce the negotiation or performance of a contract, are another example of replacing trust in people or in human-influenced processes. Smart-contracting processes are automated, but their content must be programmed first. In the future, the focus of legal questions will shift to the legal relationship between the users and the creators of corresponding algorithms. The product liability will thus gain in importance. In the area of dispute resolution processes, a displacement of classic dispute resolution instruments is to be expected because of the use of autonomous automated processes, which should be able to reduce potential disputes due to different contract interpretations or non-fulfilment (*'technical arbitration' vs. jurisdictional arbitration*). Smart contracts can reduce the role of interpersonal trust and system trust (in the functioning of the legal system) by enabling transactions to be reliably carried out without the involvement of third parties, such as trustees. The blockchain creates reliability on the transaction and is the starting point for a technical system trust, a trust in the technology, instead of a system trust in the ability and willingness of the law to be enforced and in the contractual fidelity of the contracting party. Blockchain technology and the use of

tokens based on it show the ambivalence of the new digitalisation technologies. Tokenisation may have the potential to mitigate the consequences of digital ubiquity. With the use of the decentralised and ubiquitous blockchain technology a global control of transfer processes regarding certain assets becomes possible and, in connection with smart contracts, possibly also the implementation and enforcement of licensing agreements independent of territorial instruments of law enforcement. Tokenisation could therefore be seen as a complementary instrument to 'deterritorialization'. Thus, contrary to the earlier legal scholarly discussion,[47] *it does not seem to come to a 'reterritorialization' through technology, but rather to a further 'arrangement with ubiquity'*.

4. The use of increasingly autonomous artificial intelligence in legal transactions leads to the need to either abandon the legal concept of a declaration of intent or to discuss the introduction of new concepts of legal contractual binding which are adapted to the determinacy of artificial intelligence. Since artificial intelligence cannot have a will of its own due to the lack of emotionality, the concept of a declaration of intent in a legal transaction does not fit for *algorithmic contracting*. An extension of the concept of a declaration of intent to algorithmic contracting by legal analogy is out of the question because otherwise the legal philosophical basis of private autonomy as an expression of a concept of freedom under private law would be abandoned.[48] This would be equivalent to a *capitulation of a humanistic private law to technicity*. The development of *sui generis* legal obligations which are specifically adapted to algorithmic acting is preferable.

---

[47] Torsten Bettinger and Dorothee Thum, 'Territorial Trademark Rights in the Global Village - International Jurisdiction, Choice of Law and Susbstantive Law for Trademark Disputes on the Internet, Part I', *International Review of Intellectual Property and Competition Law (IIC)* 31, no. 2 (2000): 3–6.

[48] Koos, 'Machine Acting and Contract Law – The Disruptive Factor of Artificial Intelligence for the Freedom Concept of the Private Law', *UIR Law Review* 5, no. 1 (2021): 3–9.

This would be a pragmatic adaptation of the law to digitalisation. In the long run, national private law will probably not be able to refuse this. However, this is also associated with at least a certain loss of significance of the trust concept 'contract' in favour of non-human determined forms of interaction.

5. Similar questions arise regarding the contrast of behaviour and determinacy in the competition law: The use of AI on e-commerce platforms and on social platforms, using user data collected by these platforms, affects both antitrust law as a competitive institutional protection and consumer protection law, both regarding the control of behaviour under competition law and regarding the protection of individual interests of the individual consumer. The topic has the potential to have a disruptive effect on the law because the legal concept of competitive behaviour must be adapted to market related (inter)actions of AI systems.[49] In this respect, both the algorithm-human relationship and the algorithm-algorithm relationship (collusive interaction of several algorithms to influence the market on the one hand and algorithmic based defence against other algorithmic market influences on the other hand) are affected. A market dominated by artificial intelligence no longer always presents itself as the coordination of supply and demand based on individual decisions by entrepreneurs and consumers, but rather as an increasingly automatic, logic-based, and non-human interaction of the market sides.[50] This highlights the disruptive potential and leads to a displacement of law as an instrument of controlling human behaviour in favour of technical determinism.

6. An important aspect of the change in the foundations of law through technology is the viewpoint of the concealment or displacement of accountability

[49] Koos, 'Artifical Intelligence as Disruption Factor in the Civil Law', 252.

[50] Rupprecht Podszun and Christian Kersting, 'Modernisierung des Wettbewerbsrechts und Digitalisierung', *Neue Juristische Online-Zeitschrift* 19, no. 10 (2019): 322.

through the programming and interaction of machines, which can lead to an '*organised and institutionalised irresponsibility*'.[51] If the use of AI-controlled upload filters to filter out illegal statements and information is suggested to the platform companies by the legislator, then this is an aggravation of an already problematic situation, which results from the fact that the legislator gives the control over the constitutionally[52] highly sensitive enforcement of the law into the hands of organisations whose development of power has already led to a loss of sovereignty of the states in other ways.[53] One might say that precisely *because* of the loss of control by the states over global platforms, the delegation of the duty to control to these platforms suggests itself. By doing this, the legislator includes the platforms in the responsibility in such a way that this can be implemented for them with justifiable effort. In fact, the '*responsible non-competence*'[54] of the platforms is a danger to societies. The uncertainty as to who should be responsible for illegal content on social platforms leads to a '*systematic dilution of responsibility*'.[55] It seems important that with the spread of filtering instruments based on algorithms, the

[51] This idea brought up Prof. Dr. Michael Bohne during a discussion on the topic on February 9, 2022.

[52] See the study of Felipe Romero Moreno, '"Upload Filters" and Human Rights: Implementing Article 17 of the Directive on Copyright in the Digital Single Market', *International Review of Law, Computers & Technology* 34, no. 2 (2020): 1–30.

[53] See the critic of Martin Ebers, 'Standardizing AI - The Case of the European Commission's Proposal for an Artificial Intelligence Act', in *Di Matteo/Cannarsa/Poncibò (Eds) The Cambridge Handbook of Artificial Intelligence: Global Perspectives on Law and Ethics* (Cambridge University Press, 2022), 13 towards the delegation of power to non-state-actors in the Proposal of the European Commission for an AI Regulation.

[54] Klaus-Dieter Altmeppen and Alexander Filipovic, 'Corporate Digital Responsibility. Zur Verantwortung von Medienunternehmen in digitalen Zeiten', *Communicatio Socialis* 52, no. 2 (January 2019): 7 ("*verantwortliche Nichtzuständigkeit*").

[55] Bernhard Debatin, 'Verantwortung - Grundbegriffe der Kommunikations- und Medienethik (Teil 3)', *Communicatio Socialis* 49, no. 1 (2016): 71; Altmeppen and Filipovic, 'Corporate Digital Responsibility. Zur Verantwortung von Medienunternehmen in digitalen Zeiten', 7.

still existing responsibility for the legal conformity of the platforms delegated to the companies as human conducted organizational structures is disguised. Sooner or later, this can lead to a further delegation to the non-human level and thus to a complete abolition of human responsibility. Therefore, new adapted concepts for the attribution of responsibility must already be developed now. Those concepts must also take effect when algorithms interact independently with other algorithms.

4. Lawrence Lessig's Vision in the Light of the Future Digitalization

Twenty years ago, the *Lawrence Lessig* formulated the statement "*Code is Law*".[56] *Lessig* anticipated the technical determinacy as a counterpoint to a value-oriented application of law. He described the contrast between two 'codes': The 'East Coast Code' is named after the location of the US Congress in Washington D.C.: this code is based on legislative social control oriented towards value considerations. The 'West Coast Code' is named after the location of Silicon Valley: this code is based exclusively on algorithms. The instructions are contained in software and hardware that create cyberspace.

Lessig noted that algorithms stood alongside the control of classical law as long as they were not developed and used by commercial companies. With the use of algorithms by commercial companies, the power of legislation (East Coast Code) increased, as companies can be controlled by laws.[57] This finding refers to a stage of development where algorithms are still completely controlled by individuals and by human controlled organisations. Algorithms can be used to

[56] Lessig, *Code and Other Laws of Cyberspace*, 53.
[57] Lessig, 53.

enforce corporate interests and as a means of influencing the social order, but on the other hand they can still be controlled by law insofar as there is legislative influence on the companies and their programmers. However, the influence of the legislator on the programmers of globally operating companies is decreasing due to digital globalization and growing independence of the algorithms. Programmers become lawmakers.[58] A future stronger independence of technology from direct human influence would lead to a new stage of development. Then a replacement of law by algorithms could occur, insofar as the approach to legal influence, 'behaviour', is eliminated. In the future, algorithms may no longer be merely instruments of technology companies, but autonomous factors of social and economic order alongside or even instead of law. The problem that follows from this for the future role of an ethics-based law and the humanistic foundation of law is obvious: If law were replaced by algorithmic life control, then all that would remain for the integration of ethical rules into social control would be their programming.[59] Since the corresponding programming presupposes that the programmer accepts and implements the ethical rules, there would remain a certain starting point for behavioural control through law. With increasing autonomy of the AI from the programmer, this last influence of legal behaviour control is eliminated. Ethical standards can then only influence social control from the outside. This is underlined by *Shidarta's* statement in his presentation at Universitas Diponegoro,[60] where he raised the question of the future integration of ethics and justice and where he expressed the assumption according to which the influence of ethics in the future is likely to depend on 'appeals to the ethical reason' of the technical actors.

[58] Lessig, 60.
[59] Thomas Klindt, 'Code is Law', *NJW-aktuell* 9 (2020): 3.
[60] Fn. 34.

4. Conclusion

A modern society cannot detach itself from technological development. Human decisions are prone to error and to a certain extent cannot be predicted with certainty. This distinguishes them from the determinacy of machine actions. There are areas of application in which the elimination of human error seems sensible and ethically unproblematic. On the other hand, it is characteristic of digitalisation that it is ubiquitous and eludes legal limits of the national law systems. A refusal to develop corresponding technologies would therefore not be realistic and would additionally lead to a loss of technical and economic connectivity. In general, a gradation for regulation should be made for digitalisation technologies according to their specific danger potential for society and their ethical relevance.[61] The danger potential must be analysed, not only when the technology has become established on the market, but already in the run-up to its development. Legislative measures must be pragmatically adapted to the reality of a digital globalised society so that they have a chance of being implemented by market actors. For different areas of application of such instruments, it must be decided in each case to what extent the machine determinacy as such can already represent an ethical or social problem, especially in the light of fundamental rights.

The last human point of reference of the algorithms at the level of the programmers and the technology corporations influencing them will lose significance at the latest when technology creates and reshapes itself. Whether the

[61] European Commission, 'Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS', Pub. L. No. COM(2021) 206 final 2021/0106(COD) (2021); see Ebers, 'Standardizing AI - The Case of the European Commission's Proposal for an Artificial Intelligence Act', 14–16.

humanistic basis of law, or law as a human instrument of control based on trust, will be preserved also depends on how world society stands on the social price to be paid for technological innovation. Technological progress is ambivalent:[62] it can promote productivity and prosperity, but it can also destructive and disenfranchise the individual in the interest of a collective improvement in living standards. It is possible that the role of justice and ethics is already limited to mere appeals towards the actors of the digitalisation, and that in the future determinism will replace evaluation. There are reasons to be pessimistic.

5. Acknowledgments

I thank my friend and colleague Prof. Dr. Michael Bohne from University of Applied Sciences Dortmund/Germany for numerous fruitful discussions and ideas on the topic.

6. Declaration of Conflicting Interests

None.

7. Funding

None

8. References

A. Ahlström Osakeyhtiö and others v Commission of the European Communities ('Wood Pulp'), No. 89/85 (European Court of Justice 27 September 1988).

[62] See for AI European Commission, 'White Paper on Artificial Intelligence - A European Approach to Excellence and Trust COM(2020) 65 Final', 19 February 2020, 9.

Altmeppen, Klaus-Dieter, and Alexander Filipovic. 'Corporate Digital Responsibility. Zur Verantwortung von Medienunternehmen in digitalen Zeiten'. *Communicatio Socialis* 52, no. 2 (January 2019): 202–14. https://doi.org/10.5771/0010-3497-2019-2-202.

Bär, Rolf. *Kartellrecht und internationales Kartellrecht*. Bern: Stämpfli, 1965.

Beckemper, Katharina. 'Das Rechtsgut "Vertrauen in die Funktionsfähigkeit der Märkte"'. *Zeitschrift für Internationale Strafrechtsdogmatik (ZIS)*, 2011, 318–23.

Bettinger, Torsten, and Dorothee Thum. 'Territorial Trademark Rights in the Global Village - International Jurisdiction, Choice of Law and Susbstantive Law for Trademark Disputes on the Internet, Part I'. *International Review of Intellectual Property and Competition Law (IIC)* 31, no. 2 (2000): 162–82.

Blakesley, Christopher L., and Otto Lagodny. 'Finding Harmony Amidst Disagreement Over Extradition, Jurisdiction, The Role of Human Rights, and Issues of Extraterritoriality Under International Criminal Law'. *Vanderbilt Journal of Transnational Law* 24, no. 1 (1991). https://scholars.law.unlv.edu/facpub/383.

Boehme-Neßler, Volker. 'Die Macht der Algorithmen und die Ohnmacht des Rechts. Wie die Digitalisierung das Recht relativiert'. *Neue Juristische Wochenschrift* 70, no. 42 (2017): 3031–37.

Borum, Randy. *The Science of Interpersonal Trust*. Mental Health Law & Policy Faculty Publications 574. University of South Florida, 2010. https://digitalcommons.usf.edu/mhlp_facpub/574.

Buxbaum, Hannah L. 'Territory, Territoriality, and the Resolution of Jurisdictional Conflict'. *American Journal of Comparative Law* 57 (2009): 631–75.

Darmstädter, Friedrich. 'Recht und Jurist'. *Süddeutsche Juristen-Zeitung* 3, no. 8 (1948): 318–23.

Debatin, Bernhard. 'Verantwortung - Grundbegriffe der Kommunikations- und Medienethik (Teil 3)'. *Communicatio Socialis* 49, no. 1 (2016): 68–73.

Deutsch, Jillian, and Stephanie Bodoni. 'Meta Renews Warning to E.U. It Will Be Forced to Pull Facebook'. *Time*, 8 February 2022. https://time.com/6146178/meta-facebook-eu-withdraw-data/.

Doi, Teruo. 'The Territoriality Principle of Patent Protection and Conflict of Laws: A Review of Japanese Court Decisions'. *Fordham International Law Journal* 26, no. 2 (2002). https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1874&context=ilj.

Ebers, Martin. 'Standardizing AI - The Case of the European Commission's Proposal for an Artificial Intelligence Act'. In *Di Matteo/Cannarsa/Poncibò (Eds) The Cambridge Handbook of Artificial Intelligence: Global Perspectives on Law and Ethics*. Cambridge University Press, 2022. https://dx.doi.org/10.2139/ssrn.3900378.

European Commission. Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS, Pub. L. No. COM(2021) 206 final 2021/0106(COD) (2021).

———. Regulation (EC) No. 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations (Rome II) (2021). https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32007R0864&from=EN.

———. 'White Paper on Artificial Intelligence - A European Approach to Excellence and Trust COM(2020) 65 Final', 19 February 2020. https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf.

European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (2016). https://eur-lex.europa.eu/eli/reg/2016/679/oj.

Federal Republic of Germany. Act against Restraints of Competition (GWB) (n.d.). https://www.gesetze-im-internet.de/englisch_gwb/index.html.

Fezer, Karl-Heinz. *Repräsentatives Dateneigentum - Ein zivilgesellschaftliches Bürgerrecht*. Studie der Konrad-Adenauer-Striftung e.V., 2018.

https://www.kas.de/c/document_library/get_file?uuid=f828a351-a2f6-11c1-b720-1aa08eaccff9&groupId=252038.

Fezer, Karl-Heinz, and Stefan Koos. *Internationales Wirtschaftsrecht*. 5th ed. Staudinger BGB. München: Sellier/de Gruyter, 2019.

Grupo Gigante v Dallo&Co., No. No 00-57118 (US Court of Appeals for the Ninth Circuit 15 December 2004).

Intel Corp. v European Commission ('Intel'), No. C-413/14P (European Court of Justice 6 September 2017).

Klindt, Thomas. 'Code is Law'. *NJW-aktuell* 9 (2020): 3.

Koos, Stefan. 'Artifical Intelligence as Disruption Factor in the Civil Law: Impact of the Use of Artifical Intelligence in Liability, Contracting, Competition Law and Consumer Protection with Particular Reference to the German and Indonesian Legal Situation'. *Yuridika* 36, no. 1 (2021): 235–62. https://doi.org/10.20473/ydk.v36i1.24033.

———. 'ARTIFICIAL INTELLIGENCE – SCIENCE FICTION AND LEGAL REALITY'. *Malaysian Journal of Syariah and Law* 6, no. 3 (20 December 2018): 23–29. https://doi.org/10.33102/mjsl.v6i3.135.

———. 'Digitalization of University Education and Research as Consequence of the Covid-19 Pandemic - A Paradigmatical Change'. submitted, 2021.

———. 'Global Responsibility and International Mutual Consideration in the Business Law - Theory and Reality'. In *Proceedings 6th AFHI Conference*, 21–28. Bandung: Epistema Institute, 2016.

———. 'Globalisierung, Extraterritorialität und internationalisierte sozial verantwortete Interessenverfolgung im Wettbewerbsrecht'. In *Marktkommunikation Zwischen Geistigem Eigentum und Verbraucherschutz: Festschrift für Karl-Heinz Fezer zum 70. Geburtstag*, 264–74. München: C.H.Beck, 2016.

———. 'Machine Acting and Contract Law – The Disruptive Factor of Artificial Intelligence for the Freedom Concept of the Private Law'. *UIR Law Review* 5, no. 1 (2021): 1–18. https://doi.org/10.25299/uirlrev.2021.vol5(1).6890.

———. 'Protection of Behavioural Generated Personal Data of Consumers'.

Medan: EAI, 2019. http://dx.doi.org/10.4108/eai.26-1-2019.2283267.

———. 'The Individual and the Property in Virtual Worlds'. submitted, 2022.

Lessig, Lawrence. *Code and Other Laws of Cyberspace*. New York: Basic Books, 2000. https://lessig.org/images/resources/1999-Code.pdf.

Luhmann, Niklas. *Das Recht der Gesellschaft*. 1st ed. Frankfurt am Main: Suhrkamp, 1995. https://luhmann.ir/wp-content/uploads/2021/07/Das-Recht-der-Gesellschaft.pdf.

———. *Vertrauen: Ein Mechanismus der Reduktion sozialer Komplexität*. 5th ed. Stuttgart: UTB, 2014.

Lundstedt, Lydia. *Territoriality in Intellectual Property Law - A Comparative Study of the Interpretation and Operation of the Territoriality Principle in the Resolution of Transborder Intellectual Property Infringement Disputes with Respect to International Civil Jurisdiction, Applicable Law and the Territorial Scope of Application of Substantive Intellectual Property Law in the European Union and United States*. Stockholm: Stockholm University, 2016. https://su.diva-portal.org/smash/get/diva2:972658/FULLTEXT01.pdf.

Mathur, Vishal. 'Call the Bluff: Meta Cannot and Will Not Unfriend Europe'. *Hindustan Times*, 8 February 2022. https://www.hindustantimes.com/business/call-the-bluff-meta-cannot-and-will-not-unfriend-europe-101644335650745.html.

Meessen, Karl Matthias. *Völkerrechtliche Grundsätze des internationalen Kartellrechts*. Baden-Baden: Nomos, 1975.

Peukert, Alexander. 'Territoriality and Extraterritoriality in Intellectual Property Law'. In *Handl/Zekoll/Zumbansen (Eds), Beyond Territoriality: Transnational Legal Authority in an Age of Globalization*, 189–228. Queen Mary Studies in International Law. Leiden/Boston: Brill Academic Publishing, 2012. https://ssrn.com/abstract=1592263.

Playboy Enterprises Inc. v Chuckeberry Publishing Inc., No. 939 F.Supp. 1032, 1040 (US District Court for the Southern District of New York 19 June 1996).

Romero Moreno, Felipe. '"Upload Filters" and Human Rights: Implementing Article 17 of the Directive on Copyright in the Digital Single Market'.

International Review of Law, Computers & Technology 34, no. 2 (2020): 1–30. https://doi.org/10.1080/13600869.2020.1733760.

Rupprecht Podszun, and Christian Kersting. 'Modernisierung des Wettbewerbsrechts und Digitalisierung'. *Neue Juristische Online-Zeitschrift* 19, no. 10 (2019): 321–25.

Schmidchen, Dieter. *Vertrauen und Recht: Eine ökonomische Analyse*. CSLE Discussion Paper 2000–04. Saarbrücken: Universität des Saarlandes, Center for the Study of Law and Economics (CSLE), 2000. http://hdl.handle.net/10419/23062.

Shapiro, Susan P. 'The Social Control of Impersonal Trust'. *American Journal of Sociology* 93, no. 3 (1987): 623–58.

Shidarta. 'Ethics and Law in a Digital Society - A Study of Legal Philosophy'. Presented at the 2nd International Conference on Law, Economic and Governance ICOLEG 2021, Universitas Diponegoro, 29 June 2021. https://youtu.be/Fnp90LxtVe8.

Simpson, Jeffry A. 'Chapter 25: Foundations of Interpersonal Trust'. In *Kruglanski/Higgins (Ed.) Social Psychology - Handbook of Basic Principles*, 2nd ed., 587–607. New York/London: The Guilford Press, 2007.

'Volkszählungsurteil', 1 BvR 209/83, BVerfGE 65, 1-71 (Bundesverfassungsgericht, Urteil des Ersten Senats 1983).

Welfare, Anthony. *Commercializing Blockchain - Strategic Applicationsin the Real World*. Hoboken, 2019.

Zak, Paul J., and Stephen Knack. 'Trust and Growth'. *The Economic Journal*, 2001, 295–321.

Zelger, Bernadette. 'EU Competition Law and Extraterritorial Jurisdiction – a Critical Analysis of the ECJ's Judgement in Intel'. *European Competition Journal* 16, no. 2–3 (2020): 613–27. https://doi.org/10.1080/17441056.2020.1840844.

Lex Scientia Law Review

Volume 6 Number 1 June, 2022

Author(s) Biography

Stefan Koos is Professor of Civil Law, Commercial and Business Law at the Universitaet der Bundeswehr Munich/Germany and Visiting Professor at several Indonesian universities. His research focuses on competition law, consumer protection law and international law.

How to cite (Chicago style)

Koos, Stefan. 2022. "Digital Globalization and Law". *Lex Scientia Law Review* 6 (1), 33-68. https://doi.org/10.15294/lesrev.v6i1.55092.

History of Article

Submitted: February 23, 2022
Revised: April 25, 2022
Accepted: May 23, 2022
Available online at: June 9, 2022

Lex Scientia Law Review

Volume 6 Number 1 June, 2022

We should remember that these jurisdictional issues existed when it was only paper. The cloud merely makes them bigger.

U.S. Magistrate Judge James Francis

Southern District of New York, on jurisdictional issues in e-discovery