

The Displacement of the Law by Technicity

Stefan Koos¹

¹ *Universitaet der Bundeswehr Munich, Germany*
stefan.koos@unibw.de

Abstract

Introduction to The Problem: Trust towards the legal system and interpersonal trust might lose significance and be increasingly replaced by technical determinacy following the loss of state sovereignty as a result of the deterritorialization of the law in the technical globalized world. The future evolution of artificial intelligence and digitalization may provide instruments to displace law as a social control instrument and at the same time reduce the human factor in the law.

Purpose/Objective Study: This paper is describing the connection between the ubiquity of the internet and the rise of disruptive technologies. It asks for the future role of the ethic in the legal system in a technologized society.

Paper Type: General Review

Keywords: Technicity; Digitalization; Artificial Intelligence; Territoriality Principle; Legal Ethic

Introduction

Law is a social instrument for controlling and for coordinating behaviour in the social environment. It is based on the idea of the coordination of individual interests of the single individuals of a society and, in general, on the balancing of interests of all members of the society. It's premise is a social order of human unpredictability. 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 closely related. Law and trust are therefore linked, which leads to the assumption that law loses its meaning without human trust. Trust in the legal system and interpersonal trust, for example in contractual relations, might lose its relevance and might be increasingly replaced by technical determinacy following the loss of state sovereignty as a result of the deterritorialization of the law in the internet era. As a result, law might lose its relevance as a social control instrument.

Results and Discussion

Technological Conditions of the Recent Era and the Influence of the Covid-19 Pandemic

Ubiquity of the Internet and Territoriality Principle

Independent of the Covid19 pandemic, the growth of the importance of the internet has been accompanied by a process of de-territorialisation. The internet is not limited by state borders and cannot be effectively limited to a state territory, especially not in



liberal political systems. For many years, for example, there have been struggles to develop conflict-of-law criteria in intellectual property law ([Bettinger & Thum, 2000](#)) in order to do justice to the principle of territoriality that underlies international conventions such as the TRIPS-Agreement or Art 5 (2) of the Berne Convention for the Protection of Literary and Artistic Works of 1886 ([Peukert, 2012](#)).

The location of a server from which information is uploaded to the Internet or from which rights are infringed must be irrelevant for the conflict-of-law provision of the statute. On the other hand, due to the non-existent territorial delimitability of the internet, every state connected to the internet is potentially affected by an infringement of rights on the internet and can consider its national law to be applicable under its national rules of conflict of laws. This is contrasted by the fact that state courts do not have the sovereign rights, but mostly also not the factual power, to order the removal of information from the internet with worldwide effect - extraterritorially. In this respect, one can speak of a 'crisis of the international law', which has arisen from the fact that classical conflict-of-laws-rules are based on the concept of state sovereignty and the fundamental territorial delimitability of national legal systems. This concept of order, on which the principle of territoriality, founded on the international law principle of the *courteoisie* (*comitas gentium*), is ultimately based, has come up against systematic limits as a result of the advance of the ubiquitous internet. The incompatibility between classic territorial concepts and the ubiquitous character of the digitalized society basically can no longer be compensated for with mere conceptual interpretation ([Fezer & Koos, 2019](#)).

The Covid19 pandemic has also driven and accelerated digitalisation enormously. It coincides with a phase of technological development in which further digital technologies are becoming established, some of which are likely to have a far more disruptive impact on state law than was the case in the context of the internet ([Koos, 2021c](#), p. 2). The use of evolutionarily advanced autonomously acting artificially intelligent systems may, for example, lead to a situation where the concept of 'conduct', which is essential for law and which in turn is linked to the concept of freedom in law in legal systems based on the principle of private autonomy ([Koos, 2021c](#)), is no longer sufficient to cover certain civil and business law situations. Algorithms have no 'will' and no 'desire'. They are consequently not 'free' to bind themselves in legal transactions. The same applies to the competition law, which is based on market behaviour and in its current form is no longer sufficient to satisfactorily regulate obstacles to the free competition based on harming market interactions of algorithms which are independent of human control ([Koos, 2021a](#)).

Moreover, a consequence of society's experience with digital technology during the pandemic may be the even less critical use of technology by citizens, based on the not necessarily incorrect perception that digitalisation can provide solutions not only to the current global crisis, but also to future crises. An example of this is the largely unquestioning use of video conferencing systems and the interest in virtual reality

solutions to overcome limited physical mobility. Interestingly, the pandemic thus ultimately leads to an intensification of globalisation through intensification of the phenomenon of 'technological globalisation' and thus to an effect directed against some actually reterritorialising primary effects of the pandemic (e.g. a certain negation of globalism and international cooperation and rise of national egoism). However, this technological globalisation is politically widely uncontrollable as it is based on the factuality of the technological framework conditions.

Loss of State Sovereignty as A Result of Technological Globalisation and Loss of Relevance of Law: The Capitulation of the Law to the Technological Reality

State sovereignty is limited to the own territory of a state. State law-making and law enforcement is fundamentally territorially limited. There have always been examples of extraterritorial application of law, for example in competition law. However, this has always been regarded - in addition to the aspect of practicability - as a problem of the *comitas gentium* (Buxbaum, 2009) From this principle, a self-restriction of the territorial effect of national economic law to its own state territory can be derived (Fezer & Koos, 2019). One consequence of the endeavour to limit the extraterritorial effect of the European Union market regulating law was the case law of the European Court of Justice (ECJ) not to explicitly apply the antitrust conflict of laws effect doctrine (Zelger, 2020), but to base the applicability of European antitrust law on an 'implementation of the cartel in the common market'. Even if the result of the application of this criterion ultimately corresponded to the effect doctrine, the ECJ (Intel/Commission, 2017) has only recently explicitly referred to this principle (Fezer & Koos, 2019), which was already regulated in national cartel laws (e.g. sec. 120 [2] German Act against Restraints of Competition [GWB]; see also Art. 6 [3] of the EU Rome II-Regulation). The ECJ's earlier reticence was most likely based on consideration for the principle of territoriality founded in international law (Koos, 2016a)22/07/2022 13:59:00.

With the growing worldwide interconnection of markets in the context of the globalisation (Fezer & Koos, 2019), but above all with the reduction of the importance of territorial borders in the course of virtualisation, the principle of territoriality is also losing importance (Koos, 2016b), because a territorial allocation and limitation of market effects are no longer possible in many cases (Koos, 2016a). This leads to various consequences which are relevant for the topic to be dealt with here:

1. State sovereignty is overlaid by the facticity of the virtual space. Insofar as facts take place virtually, they can indeed influence the territory of a state, but state law has only limited possibilities to handle this influence, insofar as the originator is not located on the state territory or the technical cause cannot be localised within the territory and removed. Insofar as state courts take action against such interference, their judgements basically can only relate to their own national territory. However, since the infringement on the internet is ubiquitous and cannot be territorially delimited, an injunction would be potentially territorially excessive or extraterritorial from the outset (see the case *Playboy Enterprises v.*



Chuckleberry Publishing Inc., 1996). At least the national law cannot be enforced effectively because there is no executive power beyond its own territory (*Fezer & Koos, 2019*). The same applies to the legislative regulation of protection related matters on the internet, such as data protection.

2. Some states can in fact extend their regulation beyond their own national territory and enforce it extraterritorially. This also applies to violations that take place on the ubiquitous internet. However, this is not based on the legitimacy of an extraterritorial application of the law, but rather on the factual respect of internationally operating companies addressed by regulation for the law enforcement of these states and on the interest of these companies to behave in a legally compliant manner in markets which are important for them. Politically and economically weaker states, on the other hand, have little chance of enforcing their national law on the international level. This is an example of the fact that law loses importance in the technical globalisation because principles of conflict of laws, which have been largely respected up to now, lose out to a principle of *'enforcement of the strongest'*. The principle of law actually is displaced by a *political* principle. Politically, this aspect of the *'right of the strongest'* may be justified with the viewpoint of a *'self-defence'* of the sovereign state against the otherwise uncontrollable influence from outside in virtual space. The breaking of the principle of avoiding excessive extraterritorial regulation can in this respect be understood as a direct political reaction to the decline of state sovereignty as a result of the digitalisation.

This can be illustrated by the example of the European data protection law. The European General Data Protection Regulation (GDPR) contains a provision on its extraterritorial applicability in Art. 3(2):

“2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
(b) the monitoring of their behaviour as far as their behaviour takes place within the Union.”

Regardless of the location of the data processor or of the place of processing, the connecting factor for the territorial scope of application of the GDPR is the fact that personal data of individuals in the EU are affected. Due to this connecting factor, the GDPR has a significant impact beyond the EU territory. Ultimately, this external effect of the GDPR is not based on legislative legitimacy to regulate breaches outside the EU territory, but on the connection to the domestic seat of the person affected by the breach. Basically, it can be said that the legislative right to regulate under EU law collides with the reality of the ubiquitous society because, as shown, it lacks the legal power and formally also the legal legitimacy under international law to enforce the

right to regulate against entities worldwide. Nevertheless, analogous to violations of the European competition rules, it can be stated that the GDPR is at least partially respected by companies worldwide. This seems due to the economic importance that the European internal market has for these companies.

Nevertheless, sooner or later, protecting one's own citizens on one's own territory against encroachments on their privacy interests from outside - for example, by foreign state information technology or multinational technology corporations - will be largely impossible due to the lack of territoriality of the virtual space. An example of this are augmented reality glasses, which are permanently connected to the internet and generate not only person related movement data of their users, but also data of the people who are seen through the glasses. With forthcoming technical development of those items, it may in the future not be longer visible for someone that the user of the glasses is scanning him. Thus, anybody can be observed anywhere and anytime, and person related data can be processed anytime without any control of the individual. Two things become clear here:

Firstly, future information technology could completely eliminate the data protection law concept of the individual's control over its data. High advanced scanning technology sooner or later will lead to the situation that anyone moving in the social life is potentially under surveillance permanently by others without having any option to disagree and to evade it. Secondly, the loss of state control over matters relevant to data protection law becomes apparent here, because an outflow of data to other states with a lower level of data protection or an ideologically based interest in the control of individuals in- and outside the own state territory could in fact only be prevented by a strict legal ban on respective products. Such a strict ban, however, would not be economically desirable because it would lead to an exclusion of the local market from further global technological development.

As a result, only two options remain here: Either national law insists on prohibitive regulation of the use in the field of the data protection, allowing basically the use of the items but submitting the aspect of the processing and of the transfer of data the traditional rules of data protection. Here it is quite clear that this cannot ultimately be sufficiently enforced due to the lack of enforcement power and due to the difficulties in controlling the compliant use of the items. This would mean that the law would subsequently lose significance, insofar as a law that is not or cannot be enforced is in the end replaced by other mechanisms of securing trust (Luhmann, 1995). This could be indicated by the tendency to develop 'supranationally' effective technical solutions, for example using blockchain technology and the related tokenisation.

Or the law is reshaped in a pragmatic way: With regard to data protection law, this could be done by the legislator focusing on strengthening the legal ownership of citizens of their personal data (Koos, 2019) and the self-responsibility of citizens with regard to the disclosure of their personal data instead of protective prohibitions



(Koos, 2021c). 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 infringing actions and that the state would legally accept 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 technologically globalised world has changed in comparison to the era before the internet was established in all areas of social life. On the other hand, this also means a certain 'capitulation' of the law to *technological facticity*, especially since international law in its current form is not suited to providing truly global regulatory approaches in place of the no longer sufficient national regulations.

The Displacement of the Human Factor

Law is an instrument of behavioural control. It is linked to human behaviour and social interactions (Kelsen, 1941). As long as technological actions and interactions can still be attributed to human actors, be it due to human control or at least due to an evaluative attribution of machine actions to people or human organisations, corresponding facts can still be recorded with the existing legal norms. However, the more independent from human influence machine action becomes, the less law can capture the corresponding facts. It therefore loses its significance for shaping the social framework. It will be replaced by instruments that offer security through technical measures by limiting the social effectiveness of machine actions.

An exciting example of this is the use of artificial intelligence in infiltrating malware, which makes it possible to 'behave' adaptively in the face of protective measures taken by human counteractors. In order to establish an 'equality of arms' between attacker and defender, it is to be expected that artificial intelligence will also be used on the side of the attacked party, which is equal to the deep-learning capacities of the attacker's artificial intelligence. The final consequence will be purely technical attacker-defender-interactions in which the human being is no longer actively integrated but is merely an outsider. So, it is not the law protecting network security which will be still relevant, but purely technical countermeasures.

There are various examples in which the human factor is already being displaced by technology. For example, in the competition law there is discussion about how certain actions by algorithms in markets can be legally recorded (Koos, 2021a). As long as algorithms are still directly dependent on human programming and can be attributed to companies as specific risk-creating factors, their market actions can be recorded under the current system of competition law, even if new case groups of prohibited competitive actions would have to be created for this purpose (Koos, 2021a). This will change with the increasing independence of artificial intelligence from human influence or the loss of attributability to humans.

Competition law may have to abandon the behavioural criterion at the latest then, because algorithms are acting in a determined manner and the concept of behaviour

does not fit here. The same applies to the use of artificial intelligence in the context of contractual transactions and declarations of intent. If algorithms conclude contracts independently of the control or direct programming by humans, then the corresponding circumstances can no longer be covered by the legal transaction doctrine based on the principle of private autonomy. If one constructs here a mere analogy to human declarations of will in legal transactions, one abandons the constitutional and legal philosophical basis of the doctrine of legal transactions, which manifests itself in the freedom concept of private autonomy (Koos, 2021c). Systematically, therein lies a certain 'dehumanisation' of the contract law as a consequence of a pragmatic approach to the integration of technology in the future society.

A final example of the reduction of the human factor lies in the use of artificial intelligence in filtering information to be published on the internet. Here, algorithms for social platforms alone decide which information (presumably) violates the rights of others and prevent an upload without a primary evaluative human decision. Examples of the use of such technologies are the upload filters for social media factually enforced by the EU copyright law. When algorithms decide on the freedom of expression and art, there is a considerable constitutional dimension to this (Romero Moreno, 2020).

Loss of the Importance of law in Digitalisation 5.0

Overall, various aspects can be described from which a displacement of the importance of interpersonal trust and the importance of system trust in law in the technologically globalised digital society by technicity emerges. This loss of importance of trust in the social system corresponds to a loss of importance of law in favour of control through technology.

Firstly, 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 be erroneous in the result. However, a possible 'defectiveness' of such decisions from the perspective of its impact on the human society is not based in the decision-making process itself, since defectiveness is to be defined in a normative, evaluative sense. According to this, artificial intelligence as a determined system cannot itself make erroneous decisions. However, the programming or training of the AI by humans can be faulty. At the same time, this means that the law is not yet completely superseded, because liability issues and evaluations will continue to arise at the level of technical product development and programming for the time being.

Secondly, a shift of decision-making processes relevant to fundamental rights from human decision-makers to artificial intelligence is increasingly taking place, as the example of AI filters on social media platforms shows. The tendency to transfer



evaluative decisions that are flexible and dependent on semantic aspects to algorithms is one of the consequences of the loss of control of the law, because control functions relevant to fundamental rights are being delegated from the state to the platform companies after classical legal control can no longer be exercised effectively enough in the face of the speed and ubiquity of the internet. Globally acting platforms again cannot be controlled sufficiently by the national law. Incidentally, this is also an aspect of the loss of trust in the human controllability of facts on the internet and the replacement of legal prevention directed at human behaviour with *control through technology*.

Smart contracts, computer protocols designed to digitally facilitate, verify or enforce the negotiation or performance of a contract, are a further example of the replacement of reliance on people or human-influenced processes. At the level of dispute resolution processes, a displacement of classic dispute resolution instruments is to be expected as a result of the use of autonomous automated processes that reduce the potential for disputes due to different contract interpretations or non-fulfilment (*'technical arbitration' vs jurisdictional arbitration*). Smart contracts reduce the importance of interpersonal trust or system trust (in the functioning of the legal system) in that transactions can be reliably carried out without the involvement of third parties, such as trustees. One point of connection for reliability on the transaction is the 'distributed ledger' in the blockchain. Blockchain technology is the basis of a *technical system trust* that displaces the system trust in the enforceability and willingness of the law and in the contractual fidelity of the contracting party. This technical reliability functions decentralized and ubiquitously. It therefore reduces, at least at this level (not necessarily at the programming level), the importance of national law.

Particularly important here is the connection between the advance of decentralized and ubiquitous technology-based instruments of security and the loss of the ability of national law to provide security due to the ubiquity of the internet. Luhmann's statement that law that cannot be enforced is replaced by alternative mechanisms of securing trust (Luhmann, 1995) seems to be confirmed here. The use of tokens secured in the blockchain has, in principle, the potential to bring about a mitigation of the consequences of ubiquity as a result of the internet, because the use of tokens enables global control of transmission processes with regard to certain assets. This technology thus pushes back the relevance of territorial control and law enforcement of intellectual property rights. Contrary to the jurisprudential discussion of the early 20th century (see Fezer & Koos, 2019), there is in fact not a reterritorialization using technology taking place, but rather a further 'arrangement with ubiquity', in which instruments that do not depend on state territorial enforcement gain in importance. The technology thus reinforces the deterritorialization process created before by the advance of the internet. This process is not surprising, as a technical reterritorialization of the internet seems simply not possible (Bettinger & Thum, 2000).

Conclusion

Automation and technical determinacy are increasingly displacing incentives for legally compliant behaviour. The dependence of social processes on human behaviour and human freedom of choice is increasingly reduced and replaced by technical processes. This is an important observation for the humanistic basis of law. Indeed, the effects of consistent digitalisation must be integrated into the current legal system. If law is an instrument for controlling human decisions and social interactions, then it is to be expected that incompatibilities will systematically arise to the extent that technical determinacy takes the place of human behaviour. Here, one cannot simply react with analogous conclusions from legal norms oriented towards human behaviour to determined machine actions. Care should be taken that the development of law in the digitalisation does not lead to a detachment of law from its humanistic basis in the interest of pragmatism. As a result, machine action otherwise would be granted a special position next to humans, which can lead to a conflict within the interaction between humans and machines and which disadvantage humans in their social position. This can result in a contradiction with the principle of human dignity (Koos, 2018), which represents a strict limit for the integration of technology into law that is not up for discussion by the state and society. The European Commission's approach to *'Human-centred Artificial Intelligence'* (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, 2021) is an attempt to implement this by providing for a gradation of different liability regimes in the legal assessment of the use of artificial intelligence, depending on the specific societal risks. It is motivated by the fear of the European legislator that technological development in the field of AI may displace trust (European Commission, 2020).

The displacement of law by the determinacy of technical instruments means at the same time the displacement of social justice values by effectiveness. Social responsibility and socially responsible economic law represent a strong legal-ethical component that can also be justified constitutionally via a welfare state principle (Koos, 2021b). The displacement of legal normative evaluation by technical determinism and effectiveness goals carries the danger of a loss of importance of social justice in other areas of law as well. It thus contradicts the European Commission's goal of developing a 'Human-centred' future technology. At the 2nd International Conference on Law, Economy and Governance 2021 at Diponegoro University Semarang on June 29, my colleague Shidarta emphasised the increasing importance of legal ethics in the digital society of the future (Shidarta, 2021). According to him, there is a shift from regulation by virtue of state sovereignty to monitoring and self-regulation by technology corporations. He argued that ethics in regulation by law is being replaced by utilitarianism. In order to prevent this, he stressed that the law must develop regulatory approaches before – and not after –



corresponding technical innovations that further restrict sovereignty become established in society.

This is in line with Lawrence Lessig's thesis of the relationship between 'East Coast code' (legislation) and 'West Coast code' (Silicon Valley). Lessig noted that algorithms originally stood alongside the control by classical law as long as they were not developed and used by commercial companies. With the use of algorithms by commercial corporations, the power of legislation (East Coast Code) increased as corporations can be controlled by law (Lessig, 2000). However, this finding refers to a technical stage of development in which algorithms are still controlled by individuals and human organisations. Algorithms can be used then for the enforcement of corporate interests and as a means of influencing the social order, but it can still be controlled by legal regulation. But legislative influence in the programmers of globally operating entities decreases. Programmers become 'legislators' (Lessig, 2000). A future stronger independence of technology from direct human influence would lead to a new stage of the development.

It cannot be ruled out that the process of control of law by algorithms has already led to a replacement of law by algorithms. If law were replaced by algorithmic management and control, then all that would be left for the integration of ethical rules into social management would be their programming (Klindt, 2020). Since the corresponding programming presupposes that the programmer accepts and implements the pluralistically legitimized ethical rules, there would still remain a certain starting point for behavioural control through law, which starts with the process of programming. In the future, however, algorithms may become largely autonomous factors of order alongside or instead of law.

The final human reference point of algorithms at the level of programmers and the technology corporations that influence them will lose significance at the latest when technology creates and shapes itself, for example through self-programming. Whether the humanistic basis of law or law as a human instrument of control based on trust will be preserved also depends on the position of global society on the social price to be paid for technological innovation. Technological progress is ambivalent: It can lead to an increase in global living standards, but it can also disenfranchise the individual in the interest of a collective improvement in living standards. Artificial intelligence can promote productivity and prosperity, but it can also be destructive in other respects (European Commission, 2020). It is possible that the role of justice and ethics in the governance of society is already limited to a mere appeal addressed to the technical actors, the programmers and globally operating technology corporations, and that in the future determinism will replace flexible evaluation altogether. We should be well aware of this danger.

Acknowledgment

The author thanks Dr. Shidarta from Business Law Department at Universitas Bina Nusantara Jakarta and Prof. Dr. Michael Bohne from University of Applied Sciences Dortmund for helpful discussions, as well as the editors of Jurnal Hukum Novelty for the occasion to publish this paper.

Declarations

Funding statement : None.

Conflict of interest : The author declares no conflict of interest.

Additional information : This article is the conference paper of the author for the 1st Ahmad Dahlan International Conference on Law and Social Justice (ADICoLS), August 4-5 2021 in Yogyakarta.

References

- Bettinger, T., & Thum, D. (2000). Territorial Trademark Rights in the Global Village— International Jurisdiction, Choice of Law and Substantive Law for Trademark Disputes on the Internet, part I. *International Review of Intellectual Property and Competition Law (IIC)*, 31(2), 162–182.
- Bettinger, T., & Thum, D. (2000). Territorial Trademark Rights in the Global Village— International Jurisdiction, Choice of Law and Substantive Law for Trademark Disputes on the Internet, part II. *International Review of Intellectual Property and Competition Law (IIC)*, 31(3), 285–308.
- Buxbaum, H. L. (2009). Territory, Territoriality, and the Resolution of Jurisdictional Conflict. *American Journal of Comparative Law*, 57, 631–675.
- European Commission. (2020). *White Paper on Artificial Intelligence—A European approach to excellence and trust COM(2020) 65 final*.
- Fezer, K.-H., & Koos, S. (2019). *Internationales Wirtschaftsrecht* (5th ed.). Sellier/de Gruyter.
- Intel/Commission, C-413/14 (ECJ 6 September 2017).
- Kelsen, H. (1941). The Law as a Specific Social Technique. *University of Chicago Law Review*, 9(1), 75–97.
- Klindt, T. (2020). Code is Law. *NJW-Aktuell*, 9, 3.
- Koos, S. (2016a). Globalisierung, Extraterritorialität und internationalisierte sozial verantwortete Interessenverfolgung im Wettbewerbsrecht. In *Marktkommunikation zwischen geistigem Eigentum und Verbraucherschutz: Festschrift für Karl-Heinz Fezer zum 70. Geburtstag* (pp. 264–274). C.H.Beck.
- Koos, S. (2018). Artificial Intelligence – Science Fiction and Legal Reality. *Malaysian Journal of Syariah and Law*, 6(3), 23–29. <https://doi.org/10.33102/mjsl.v6i3.135>
- Koos, S. (2019). *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.



- Koos, S. (2021a). Artificial Intelligence as Disruption Factor in the Civil Law: Impact of the use of Artificial Intelligence in Liability, Contracting, Competition Law and Consumer Protection with Particular Reference to the German and Indonesian Legal Situation. *Yuridika*, 36(1), 235–262. <https://doi.org/10.20473/ydk.v36i1.24033>
- Koos, S. (2021b). Consistency and Law Comparison in Consumer Protection Law Design in the Light of the Socially Responsible Market Economy Approach. *Indonesian Journal of Economics, Social and Humanities*, 3(2), 97–104.
- Koos, S. (2021c). Machine Acting and Contract Law – The Disruptive Factor of Artificial Intelligence for the Freedom Concept of the Private Law. *UIR Law Review*, 5(1), 1–18. [https://doi.org/10.25299/uirlrev.2021.vol5\(1\).6890](https://doi.org/10.25299/uirlrev.2021.vol5(1).6890)
- Koos, S. (2016b). Global Responsibility and International Mutual Consideration in the Business Law—Theory and Reality. *Proceedings*, 21–28.
- Lessig, L. (2000). *Code and Other Laws of Cyberspace*. Basic Books.
- Luhmann, N. (1995). *Das Recht der Gesellschaft* (1st ed.). Suhrkamp.
- Peukert, A. (2012). Territoriality and Extra-Territoriality in Intellectual Property Law. In *Beyond Territoriality—Transnational Legal Authority in an Age of Globalization* (Vol. 11, pp. 189–228). Martinus Nijhoff Publ.
- Playboy Enterprises v. Chuckleberry Publishing Inc., 39 USPQ 2d 1746 (Southern District Court of New York 19 June 1996).
- 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, no. COM/2021/206 final (2021).
- Romero Moreno, F. (2020). ‘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(2), 1–30. <https://doi.org/10.1080/13600869.2020.1733760>
- Shidarta. (2021, June 29). *Ethics and Law in a Digital Society—A Study of Legal Philosophy*. 2nd International Conference on Law, Economic and Governance ICOLEG 2021, Universitas Diponegoro. <https://youtu.be/Fnp90LxtVe8>
- Zelger, B. (2020). EU Competition law and extraterritorial jurisdiction – a critical analysis of the ECJ’s judgement in Intel. *European Competition Journal*, 16(2–3), 613–627. <https://doi.org/10.1080/17441056.2020.1840844>