Int. Cybersecur. Law Rev. (2021) 2:203–208
https://doi.org/10.1365/s43439-021-00039-2

EDITORIAL

Editorial

Dennis-Kenji Kipker

Accepted: 15 September 2021 / Published online: 30 September 2021

1 Dear reader,

Data flows do not stop at national borders—but that is nothing new. What is relatively new, however, is that the IT law of a national legislature also increasingly does not stop at its own national borders—this is what is known as the "extraterritorial effect" of laws. For Europe, this extraterritorial effect of IT-related legislation, even outside of pure business law or antitrust legislation, has gained widespread attention since 2016 at the latest with the General Data Protection Regulation (GDPR). In this way, concepts such as the "market location principle" mean that foreign companies based in other countries must also adapt more and more to European law in the design of their IT processes if they want to develop business activities in the EU. With the general global consolidation of IT regulation that we are currently seeing and have seen increasingly in recent years, the extraterritorial effect of laws is also more and more affecting cybersecurity law. The Chinese legislature in particular regularly creates uncertainty for foreign companies with business activities in the People's Republic of China by not only continuously enacting new laws with an IT security focus—such as the Cryptography Law and the Data Security Law—directly following the Chinese Cybersecurity Law from 2016, but also interpreting existing regulations in the often general clause-like formulations of current IT security legislation in such a way that they can have a global extraterritorial effect. This currently includes, for example, attempts to require manufacturers to first disclose zero-day vulnerabilities to Chinese authorities before they can be published via other disclosure procedures.

The last example in particular proves that the actual impact of extraterritorial IT legislation is enormous and can ultimately even become a prerequisite for market ac-

Dennis-Kenji Kipker (✉)
Universität Bremen, Bremen, Germany
E-Mail: kipker@uni-bremen.de

cess—or should at least be observed from a compliance perspective in order to avoid fines, claims for damages and government sanctions. Even if the Chinese legislature is often used as an example to demonstrate the increasingly strong extraterritoriality of IT legislation, it is by no means alone—and more and more countries are coming up with new regulations. For example, IT security regulations that also have an effect abroad can now be found in Indian law, in U.S. law and in Russian legislation and, with the new IT Security Act 2.0 (IT-SiG 2.0), not least also in German legislation when it comes to guarantee declarations and international supply chain proofs for secure IT products. In some cases, such regulations are also linked to far-reaching data localization obligations in order to ensure the value and protection of (personal) data as a national security interest.

Extraterritorial laws in IT are, so to speak, "in vogue" and are increasingly becoming a means of exerting pressure in terms of economic policy, not only to control foreign companies and transnationally active large corporations, but also to play off one's own economic power on the international stage. National state security interests also play a role, as noted earlier. An interesting effect of extraterritorial IT legislation with the market location principle is also that states align their own national law with the corresponding foreign laws with their international impact. The best example in this context is the new Chinese "Personal Information Protection Law" (PIPL), which recently came into force on November 1, 2021 and has transferred numerous principles from the European General Data Protection Regulation into national Chinese law, but without necessarily pursuing the same regulatory objectives as the EU legislator. Consequently, if a state or an association of states has considerable market power, economic policy considerations in an international context can certainly influence national legislation. And, of course, this also applies beyond IT and cybersecurity.

However, companies affected by foreign IT laws are mostly left alone to find and correctly interpret the legal provisions that apply to them, as well as to collect any necessary contacts with authorities for implementation. Language and cultural barriers further complicate dealing with foreign IT compliance requirements. Small and medium-sized enterprises (SMEs) in particular face considerable problems here. In addition, the legal and political spheres overlap, as there is no clear point of contact or problem solver for the dilemma of foreign impact of international IT legislation: Should the legal counsel directly be addressed, or is it better to rely on the influence of industry associations, chambers of commerce, or national ministries to engage in dialogue with the relevant states? There is certainly no panacea here—just as the last word has probably not yet been spoken in this still open question and challenge for international IT compliance.

As a result, however, it can at least be stated that it makes more and more sense to deal with foreign legislation in a global context—also beyond the law of IT security—in order to continue to offer products and services in line with the market. This issue of the ICLR is once again intended to help with this task, among other things, and contains various current and interesting contributions and topics "around the globe": For example, one focus in this issue is the draft for a new EU NIS-2 Directive, which is examined from different perspectives by the authors of two articles. There are also news with regard to China, which was already mentioned

at the beginning of this editorial. These are presented in the article on the new Chinese data security law with a practical perspective. Other international papers provide an overview of the legal basis for cybersecurity in Russia and India's new legislation on platform regulation, which is also relevant from a security perspective. Several articles in this issue also take a closer look at Germany in terms of criminal law in dealing with criminal trading platforms on the Internet and the latest relevant legislation, as well as portscans in the light of civil law claims. Going beyond purely legal considerations, another paper presents the depths and shallows of "Open Source Intelligence" (OSINT), which can be used, among other things, to prepare for cyber attacks. Finally, we venture a look "across the pond" with a paper that compares and analyzes the German and Brazilian (constitutional) legal guarantees for IT security. Last but not least, this issue introduces a new section, "Numbers & Statistics," which records data breaches numerically, breaks them down by different countries, and evaluates them.

As always, I hope you enjoy reading the latest issue of the International Cybersecurity Law Review. If you have any questions, please do not hesitate to contact the authors of the articles directly—and feel invited to contribute your own article to one of the upcoming issues if you are currently working on an internationally relevant topic of cybersecurity regulation that might be of interest to the readership.

Best regards from the Hanseatic City of Bremen/Germany,

Prof. Dr. Dennis-Kenji Kipker

2 Liebe Leserin, lieber Leser,

Datenströme machen nicht an den Grenzen von Staaten halt – das ist aber nichts Neues. Verhältnismäßig neu ist jedoch, dass auch das IT-Recht eines nationalen Gesetzgebers immer weniger an den eigenen Staatsgrenzen endet – hierbei handelt es sich um die sogenannte „extraterritoriale Wirkung" von Gesetzen. Für Europa hat diese Auslandswirkung von IT-bezogenen Rechtsvorschriften auch außerhalb reiner Wirtschaftsrechts- bzw. Kartellrechtsgesetzgebung spätestens seit 2016 mit der Datenschutz-Grundverordnung breite Aufmerksamkeit erlangt. Begriffe wie das „Marktortprinzip" führen auf diese Weise dazu, dass sich ausländische Unternehmen mit Sitz in anderen Staaten auch in der Gestaltung ihrer IT-Prozesse mehr und mehr auf das europäische Recht einstellen müssen, wenn sie eine Geschäftstätigkeit in der EU entfalten wollen. Mit der allgemeinen globalen Verdichtung der IT-Regulierung, die wir aktuell und in den letzten Jahren zunehmend feststellen können, betrifft die extraterritoriale Wirkung von Gesetzen immer mehr auch das Recht der Cybersicherheit. So sorgt insbesondere der chinesische Gesetzgeber regelmäßig für Unsicherheit bei ausländischen Unternehmen mit Geschäftstätigkeit in der Volksrepublik China, indem er in direktem Anschluss an das Chinese Cybersecurity Law aus 2016 nicht nur laufend neue Gesetze mit IT-Sicherheitsbezug erlässt – so zum Beispiel das Cryptography Law und das Data Security Law – sondern bestehende Regelungen in den oftmals generalklauselartig formulierten Vorschriften aktueller IT-Sicherheitsgesetzgebung so auslegt, dass sie eine globale extraterritoriale Wirkung entfalten können. Hierzu zählen aktuell beispielsweise auch Vorstöße, dass Zero-Day-

Schwachstellen von Herstellern zunächst an chinesische Behörden zu übermitteln sind, bevor sie über sonstige Disclosure-Verfahren publiziert werden dürfen.

Gerade letztes Beispiel belegt, dass die faktische Wirkkraft extraterritorialer IT-Rechtsvorschriften enorm ist und letzten Endes gar zu einer Markzugangsvoraussetzung werden kann – oder aber zumindest unter Compliance-Gesichtspunkten beachtet werden sollte, um Bußgelder, Schadensersatzansprüche und staatliche Sanktionen zu vermeiden. Auch wenn der chinesische Gesetzgeber oftmals als Beispiel herangezogen wird, um die immer stärker werdende Extraterritorialität der IT-Rechtsetzung zu belegen, so ist er längst nicht allein – und es treten immer weitere Staaten mit neuen Regelungen auf den Plan. So finden sich IT-sicherheitsrechtliche Vorschriften, die auch im Ausland ihre Wirkung entfalten, mittlerweile im indischen Recht, im US-amerikanischen Recht sowie in russischen Rechtsvorschriften und mit dem neuen IT-Sicherheitsgesetz 2.0 nicht zuletzt auch in der deutschen Gesetzgebung wieder, wenn es um Garantieerklärungen und internationale Lieferkettennachweise für sichere IT-Produkte geht. Teilweise sind solcherlei Regelungen auch mit weitreichenden Datenlokalisierungspflichten verbunden, um Werthaltigkeit und Schutz (personenbezogener) Daten als nationales Sicherheitsinteresse zu gewährleisten.

Extraterritoriale Gesetze in der IT sind sozusagen „en vogue“ und werden mehr und mehr in wirtschaftspolitischer Hinsicht zu einem Druckmittel, um nicht nur ausländische Unternehmen und transnational agierende Großkonzerne zu steuern, sondern auch, um die eigene Wirtschaftsmacht auf dem internationalen Parkett auszuspielen. Nationale staatliche Sicherheitsinteressen spielen dabei wie zuvor angemerkt ebenfalls eine Rolle. Eine interessante Wirkung der extraterritorialen IT-Rechtsetzung mit dem Marktortprinzip ist auch, dass Staaten ihr eigenes nationales Recht an die entsprechenden ausländischen Gesetze mit ihrer internationalen Wirkkraft angleichen. Bestes Beispiel ist in diesem Zusammenhang das neue chinesische Datenschutzgesetz „Personal Information Protection Law“ (PIPL), das jüngst zum 1. November 2021 in Kraft trat und zahlreiche Prinzipien aus der europäischen Datenschutz-Grundverordnung in nationales chinesisches Recht übertragen hat, ohne dabei jedoch zwingend dieselben regulatorischen Ziele wie der EU-Gesetzgeber zu verfolgen. Wenn folglich ein Staat oder ein Zusammenschluss von Staaten über eine erhebliche Marktmacht verfügt, so können wirtschaftspolitische Erwägungen im internationalen Kontext die nationale Rechtsetzung durchaus beeinflussen. Und das gilt selbstredend auch jenseits von IT und Cybersecurity.

Von den ausländischen IT-Gesetzen betroffene Unternehmen sind jedoch zumeist allein damit gelassen, die für sie geltenden Rechtsvorschriften ausfindig zu machen und richtig zu interpretieren, sowie eventuell notwendige Behördenkontakte zur Umsetzung auszukundschaften. Sprachliche und kulturelle Barrieren erschweren den Umgang mit ausländischen IT-Compliance-Vorgaben weiter. Gerade für die kleinen und mittelständischen Unternehmen (KMU) kommt es hier zu erheblichen Problemen. Hinzu tritt, dass sich die rechtliche und die politische Sphäre überschneiden, da es keinen klaren Ansprechpartner oder Problemlöser für das Dilemma ausländischer Wirkung der internationalen IT-Rechtsetzung gibt: Sollte man sich eher an den juristischen Beistand wenden, oder besser auf die Einflussnahme von Branchenverbänden, Industrie- und Handelskammern oder nationalen Ministerien vertrauen,

die in Dialog zu den entsprechenden Staaten treten? Mit Sicherheit gibt es hier nicht das Allheilmittel – genauso wenig, wie in dieser noch offenen Frage und Herausforderung für die internationale IT-Compliance bereits das letzte Wort gesprochen sein dürfte.

Im Ergebnis kann aber zumindest festgehalten werden, dass es mehr und mehr Sinn macht, sich mit der ausländischen Rechtsetzung in einem globalen Kontext – auch jenseits des Rechts der IT-Sicherheit – auseinanderzusetzen, um auch in Zukunft nicht nur marktgerechte, sondern ebenso marktkonforme Produkte und Dienstleistungen anzubieten. Auch diese Ausgabe des ICLR soll unter anderem wieder bei der Bewältigung dieser Aufgabe helfen und hält verschiedene aktuelle und interessante Beiträge und Themen „rund um den Globus" bereit: So bildet ein Schwerpunkt in diesem Heft der Entwurf für eine neue NIS-2-Richtlinie der EU, der von den Verfasserinnen und Verfassern zweier Beiträge aus unterschiedlichen Perspektiven beleuchtet wird. Auch mit Blick auf das eingangs schon angesprochene Thema China gibt es Neuerungen, die im Aufsatz zum neuen chinesischen Data Security Law mit Sichtweise aus der Praxis vorgestellt werden. Weitere internationale Paper geben einen Überblick über die rechtlichen Grundlagen zur Cybersicherheit in Russland und über die neue indische Gesetzgebung zur Plattformregulierung, die auch mit Blick auf Sicherheitsaspekte Relevanz besitzt. Verschiedene Beiträge in dieser Ausgabe vertiefen überdies den Blick nach Deutschland zu den Themen strafrechtlicher Umgang mit kriminellen Handelsplattformen im Internet und der neuesten einschlägigen Gesetzgebung sowie zu Portscans im Lichte zivilrechtlicher Anspruchsgrundlagen. Über die rein rechtliche Betrachtung hinausgehend stellt ein weiteres Paper die Tiefen und Untiefen von „Open Source Intelligence" (OSINT) vor, die unter anderem zur Angriffsvorbereitung verwendet werden kann. Den Blick „über den großen Teich" wagen wir schließlich mit einem Aufsatz, der die deutschen und brasilianischen (verfassungs)rechtlichen Gewährleistungen zur IT-Sicherheit gegenüberstellt und analysiert. Last but not least wird mit diesem Heft eine neue Rubrik „Numbers & Statistics" eingeführt, die Data Breaches zahlenmäßig erfasst, nach unterschiedlichen Staaten aufschlüsselt und bewertet.

Wie immer wünsche ich Ihnen eine erkenntnisreiche und interessante Lektüre der neuesten Ausgabe des „International Cybersecurity Law Review". Nehmen Sie bei Fragen gerne direkten Kontakt zu den Autorinnen und Autoren der Beiträge auf – und fühlen Sie sich eingeladen, auch selbst einen Beitrag für eine der kommenden Ausgaben beizusteuern, sollten Sie sich aktuell mit einem durchaus auch international relevanten Thema der Cybersecurity-Regulierung beschäftigen, das für die Leserschaft von Interesse sein könnte.

Mit den besten Grüßen aus der Hansestadt Bremen,
Prof. Dr. Dennis-Kenji Kipker

Funding Open Access funding enabled and organized by Projekt DEAL.

Dennis-Kenji Kipker