Dear reader,

I am pleased to present you with the first issue of *International Cybersecurity Law Review* (ICLR) for 2022, as the new General Editor of the journal. The ICLR journal was founded two years ago with the mission to reflect the increasing number of legal regulations on cyber security in a practical, up-to-date, and clear manner. We strive to make cybersecurity, a complex interdisciplinary topic between law and technology, easily accessible to legal practitioners and experts working in the IT sector. In times of increasing threats to the security of IT infrastructures, it has become obvious that tackling the threats to digitalisation requires a mix of technological and legal safeguards.

One of the cornerstones of today’s digitisation is semiconductor chips, which are at the core of any connected item. For years now, major economies around the world have sought to promote and attract semiconductor manufacturers to meet the increased demand of chips across sectors. The COVID-19 crisis has put enormous pressure on supply chains generally but more specifically so on the chip sector. For example, in the automotive industry in Europe the lack of supply chain security has led to significant production losses. While the car industry and consumer electronics are affected by the unsecure supply chains of semiconductor chips, many other industries that make up the critical infrastructures of our societies like healthcare, energy supply, space and aviation, and telecommunications are also affected.

In Europe, the EU Commission is now addressing the situation with its proposal for an EU “Chips Act”. The EU Chips Act is an industrial policy instrument that is intended to make it more attractive for investors to set up semiconductor production plants in Europe. The proposal shows promise, as shortly after it was published, the
US chip manufacturer Intel announced that it would invest €17 billion in a new factory in Germany and another €16 billion in other sites across Europe.

In addition to the attractive investment-driven aspects and the aim of making Europe less dependent on the volatile chip market, the EU Chips Act also deals with improving the security of semiconductor chips. It proposes that chips are certified—from the value chain to integration in end products—and that this is considered in public procurement. It also seeks to promote international standardisation of semiconductor chips.

Certification schemes for trusted and secure chips will be introduced for sectors and technologies where there is a potentially high social impact, which respectively raises the significance of security. A newly established European Semiconductor Board has been tasked with assisting the EU Commission in identifying and prioritising the sectors and products that require trustworthy chips, which includes consulting the relevant private stakeholders. This all bears in mind the legal requirements from harmonised Union legislation and the relevant activities within the European cybersecurity certification framework.

Cybersecurity certification frameworks is a topic that has been examined in two papers in our current issue of the ICLR. The paper “European cybersecurity certification schemes and cybersecurity in the EU internal market” analyses the possibilities of certification under the EU Cybersecurity Act and sheds light on the appropriateness of the minimum-security targets set out in the Act to support organisations in defending against and dealing with cyber threats. The paper on the draft European AI Regulation addresses the (so far) missed opportunity for coordination and mutual recognition of cybersecurity certifications under the AI Regulation and the EU Cybersecurity Act.

Another focus of our issue is the healthcare and life science sectors, which are technologically well advanced and digitised. As the article on cybersecurity in hospitals very rightly points out, IT compliance in hospitals should sit with the board. Another hot topic is the use of artificial intelligence and algorithm-based decisions in everyday medical treatment. The highly topical article on the example of ‘Dr. Algorithm’ looks at how the law should react to the adoption of algorithm-based decisions and whether new regulatory approaches to risk assessment are needed.

This issue also explores the question of the effectiveness of cybersecurity governance, which is addressed in a global study that analyses the results of various national cybersecurity governance concepts from the last five years. Another article delves into the cybersecurity ecosystem in Europe and provides an overview of existing regulations and identifies possible gaps.

Finally, with a look across the pond, an article explains the US Department of Justice’s new initiative against fraud in cyberspace. The initiative aims to use civil remedies to hold government contractors accountable for using US information or data that is at risk of cybersecurity fraud.

On behalf of the entire editorial team and the Scientific Advisory Board, to which we welcome many new experts from around the world, I wish you an enlightening and enjoyable read.

With best wishes,

Julia Utzerath
Liebe Leserin, lieber Leser,

ich freue mich, Ihnen in meiner neuen Rolle als General Editor die erste Ausgabe des *International Cybersecurity Law Review* (ICLR) für das Jahr 2022 vorstellen zu dürfen. Die Zeitschrift ICLR ist vor zwei Jahren mit dem Auftrag angetreten, die steigende Vielzahl an rechtlichen Regularien im Bereich Cybersicherheit praxisnah, aktuell und übersichtlich wiederzugeben. Es ist uns gelungen, die interdisziplinäre Natur des Themas mit seiner Mischung aus Recht und Technologie sowohl für den Rechtspraktiker als auch holistisch für jeden, der im IT-Sektor tätig ist, aufzuarbeiten. Denn in Zeiten zunehmender Bedrohung der Sicherheit der IT-Infrastrukturen zeigt es sich mehr denn je, dass die erfolgreiche Digitalisierung nur mit einem Mix aus technischem Fortschritt gepaart mit rechtlicher Absicherung gelingen kann.

Hinzu kommt seit dem Beginn der Coronakrise der sich weiter verstärkende geopolitische Druck auf die Sicherheit der Versorgung mit IT-spezifischer Technik wie Halbleiterchips, den sogenannten „Building Blocks“ der Digitalisierung. Schon seit Jahren bemühen sich die großen Volkswirtschaften weltweit um die Förderung und Ansiedlung von Halbleiterherstellern, um der sorglosen und steigenden Nachfrage gerecht zu werden. Zudem ist der Druck auf die Lieferketten durch die Coronakrise auch im Chip-Sektor enorm gestiegen. Wir haben zum Beispiel in der Autoindustrie in Europa erlebt, wie fehlende Lieferkettensicherheit zu erheblichen Produktionsausfällen führen kann. Von der Verfügbarkeit der Halbleiterchips sind nicht nur Unterhaltungselektronik und Autoindustrie betroffen, sondern viele Industriezweige, die Teil der kritischen Infrastrukturen unserer Gesellschaften sind, wie das Gesundheitswesen, die Energieversorgung, die Raum- und Luftfahrt und natürlich die Telekommunikation, um nur einige zu nennen.

Diesem trägt in Europa nun die EU-Kommission mit dem Vorschlag eines EU „Chips Acts“ Rechnung, einem industriepolitischen Instrument, das die Ansiedlung von Halbleiterproduktionen in Europa für Investoren attraktiv machen soll. Ein Vorschlag, der erfolgsversprechend erscheint: Kurz nach Veröffentlichung des EU Chips Acts gibt der US-amerikanische Chiphersteller Intel bekannt, 17 Mrd. € in eine neue Fabrik in Deutschland und weitere 16 Mrd. € in andere europäische Standorte zu investieren.

Neben den investitionsgetriebenen Aspekten und dem Ziel, Europa unabhängiger von geopolitischen Spannungen auf dem Chip-Markt zu machen, enthält der EU Chips Act auch Überlegungen zur Verbesserung der Sicherheit von Halbleiterchips. Hier zeigt sicher wieder die Verzahnung mit unserem Thema der Cybersicherheit. Die Zertifizierung der Chips soll von der Wertschöpfungskette bis zur Integration in Endprodukte erfolgen und sowohl bei der Vergabe öffentlicher Aufträge berücksichtigt als auch in internationalen Normungstätigkeiten gefördert werden. Es ist geplant, Zertifizierungsverfahren für vertrauenswürdige und sichere Chips in Sektoren und für Technologien einzuführen, die potenziell von hoher sozialer Bedeutung sind, was wiederum die Bedeutung ihrer Sicherheit entsprechend erhöht.

Welche Sektoren und Technologien im Einzelnen unter die Zertifizierungsvorgaben fallen, soll von der EU-Kommission mit Hilfe des neu zu etablierenden europäischen Halbleiter-Ausschusses (European Semiconductor Board) und unter Einbeziehung der verschiedenen Stakeholder und Initiativen festgelegt werden. Es
sollen diejenigen Sektoren und Produkte, die aufgrund ihrer hohen sozialen Bedeutung vertrauenswürdige Chips benötigen, ermittelt und priorisiert werden. Dies soll unter Berücksichtigung der rechtlichen Anforderungen aus harmonisierten Unionsrechtsvorschriften und des europäischen Cybersicherheitszertifizierungsrahmens geschehen.

Der Frage, welcher Zertifizierungsrahmen für eine adäquate Cybersicherheit nötig und möglich ist, widmen sich in unserem aktuellen Heft gleich zwei Beiträge. Das Paper „European Cybersecurity Certification Schemes and cybersecurity in the EU internal market“ analysiert die Möglichkeiten der Zertifizierung unter dem EU Cybersecurity Act und beleuchtet, wie angemessen die dort aufgestellten Mindestsicherheitsziele sind, um Organisationen bei der Abwehr von und dem Umgang mit Cyberbedrohungen zu unterstützen. Der Beitrag zum Entwurf der europäischen KI-Verordnung thematisiert die (bisher) verpasste Gelegenheit zur Koordinierung und gegenseitigen Anerkennung der Cybersicherheitszertifizierungen im Rahmen der KI-Verordnung und dem EU Cybersecurity Act.

Ein weiterer Schwerpunkt dieses Hefts liegt auf Fragen rund um den Gesundheitssektor als einem Bereich, dessen Technisierung und Digitalisierung bereits weit fortgeschritten ist und der, wie der Beitrag zur Cybersicherheit im Krankenhaus beleuchtet, die Einordnung der IT-Compliance als Leistungsaufgabe erfordert. Ein weiterer aktueller Aspekt im Gesundheitswesen ist der Einsatz von künstlicher Intelligenz und algorithmenbasierten Entscheidungen, die in den ärztlichen Behandlungsalltag Einzug gehalten haben. Wie das Recht auf diese neuen Anwendungsfälle reagieren soll und ob es neuer Regelungsansätze zur Risikoabschätzung bedarf, um den ärztlichen Behandlungsstandards und Haftungsfragen ausreichend Rechnung zu tragen, wird in einem weiteren spannenden wie gleichermaßen hochaktuellen Beitrag aufgearbeitet.

Weiterhin finden sich aktuelle Themen wie die Frage der Effektivität von Cybersecurity Governance in diesem Heft, angereichert durch eine Studie, die die Ergebnisse diverser nationaler Cybersecurity-Governance-Konzepte der letzten fünf Jahre im globalen Überblick analysiert. Ein weiterer Beitrag widmet sich dem Ökosystem der Cybersicherheit in Europa und gewährt einen Überblick über die aktuell bestehenden Regulierungen und etwaigen Lücken.

Abschließend wird „mit Blick über den großen Teich“ in einem Beitrag die neue Initiative des US Department of Justice gegen Betrug im Cyberspace erläutert, deren Ziel es ist, mit Hilfe zivilrechtlicher Rechtsmittel staatliche Auftragnehmer zur Rechenschaft zu ziehen, die US-Informationen oder -Daten durch Cybersicherheitsbetrug in Gefahr bringen.

Ich wünsche Ihnen im Namen des gesamten Herausgeberteams sowie des wissenschaftlichen Beirats, in dem wir eine Vielzahl neuer Expertinnen und Experten aus verschiedensten Ländern rund um den Globus begrüßen dürften, eine aufschlussreiche und unterhaltsame Lektüre.

Mit den besten Wünschen
Julia Utzerath

Hinweis des Verlags Der Verlag bleibt in Hinblick auf geografische Zuordnungen und Gebietsbezeichnungen in veröffentlichten Karten und Institutsadressen neutral.
