BURKARDT & PARTNER
RECHTSANWÄLTE
上 海 申 欧 律 师 事 务 所

ROOM 1706 · FIVE CORPORATE AVENUE · 150 HUBIN ROAD
HUANG PU DISTRICT · SHANGHAI 200021 · P.R. CHINA
中国上海市黄浦区湖滨路150号企业天地5号楼1706室 邮编 200021
电话 PHONE +86 (21) 6321 0088 传真 FACSIMILE +86 (21) 6321 1100
Info@BKTlegal.com www.BKTlegal.com

Anti-Spionage-Gesetz: bringt die Novelle zusätzliche Risiken für Ihre Tätigkeit in China?

Datum: 18. Januar 2024

Wie Sie dem Datum dieses Beitrags entnehmen können, waren wir anfänglich der Meinung, dass eine Kommentierung der am 1. Juli 2023 in Kraft getretenen Novelle des Anti-Spionage-Gesetzes der Volksrepublik China („Anti-Spionage-Gesetz“ oder „Novelle“) für unsere Mandanten nicht von gesteigertem Interesse ist. Aufgrund der großen medialen Aufmerksamkeit, welche das Anti-Spionage-Gesetz erfahren hat, als auch aufgrund zahlreicher Anfragen unserer Mandanten und Medien (ORF-Interview mit Rainer Burkardt zu diesem Thema) haben wir uns nun doch entschlossen, Ihnen unsere Sichtweise auf die Novelle mitzuteilen, auch um eventuell bestehenden Bedenken zu begegnen.

Seit der Verabschiedung der Novelle am 26. April 2023 sorgt diese für Diskussionen und Verunsicherung insbesondere bei Vertretern von ausländisch-investierten Unternehmen in China, die eigene Unternehmensdaten oder Daten Dritter sammeln und ins nicht-chinesische Ausland übertragen. Im Folgenden möchten wir der Frage nachgehen, ob die Novelle, wie von vielen befürchtet, für ausländisch-investierte Unternehmen zusätzliche Risiken mit sich bringt, und geben unsere Empfehlungen zur Risikominimierung.

Zunächst stellt sich bei einer Gesetzesinterpretation die Frage, zu welchem Zweck das Gesetz vom Gesetzgeber erlassen bzw. novelliert wurde. Laut dem Bericht des Verfassungs- und Rechtsausschusses des Nationalen Volkskongresses über die Ergebnisse seiner Beratungen zum Anti-Spionage-Gesetz vom 27. April 2023 soll die Novelle neben den “traditionellen“ auch “nicht-traditionelle Sicherheitsbedrohungen“ bekämpfen. Damit zielt die Novelle insbesondere auf Cyberangriffe auf kritische Informationsinfrastrukturen, da diese zum Zeitpunkt des Erlasses des Anti-Spionage-Gesetzes am 1. November 2014 wegen der damals noch geringeren Vernetzung keine so große Bedrohung wie heute darstellten.

Ursprünglich wurde das Anti-Spionage-Gesetz mit insgesamt 40 Artikeln erlassen, welche sich in fünf Kapiteln gliederten: Kapitel I: Allgemeine Bestimmungen; Kapitel II: Befugnisse der Organe der Staatssicherheit für die Spionageabwehr; Kapitel III: Pflichten und Rechte der Bürger und Organisationen; Kapitel IV: Haftung und Kapitel V: Ergänzende Bestimmungen.

Das erstmalig novellierte Anti-Spionage-Gesetz hat heute mit 71 Artikeln fast die doppelte Länge und gliedert sich in sechs Kapitel.

- Kapitel I: Allgemeine Bestimmungen
- Kapitel II: Sicherheitsvorkehrungen (vorher Kapitel III: Pflichten und Rechte der Bürger und Organisationen): enthält neue Bestimmungen zu Präventivmaßnahmen zur Spionageabwehr sowie zur staatlichen und behördlichen Koordination und Kontrolle der Anti-Spionage-Maßnahmen.

- Kapitel III: Untersuchung und Behandlung (vorher Kapitel II: Befugnisse der Sicherheitsbehörden für die Spionageabwehr): sieht nun mehrere, detailliert formulierte Befugnisse und Pflichten der Anti-Spionage-Behörden bei der Untersuchung und Behandlung von Spionageaktivitäten vor.
- Kapitel IV: Schutz und Überwachung: dieses neu hinzugefügte Kapitel hat die vorher in anderen Kapiteln vorhandenen Bestimmungen (z.B. die Behördenbefugnis, nach Vorlage entsprechender Dokumente Räumlichkeiten zu betreten und Archive, Materialien oder Gegenstände zu besichtigen) übernommen und sieht u.a. neue Regelungen zur Entschädigung für die durch behördliche Anti-Spionage-Maßnahmen entstandenen Schäden sowie Regelungen zur behördeninternen Überwachung vor.
- Kapitel V: Haftung: sieht neue Sanktionen vor
- Kapitel VI: Ergänzende Bestimmungen

Im Folgenden werden einige inhaltliche Änderungen vorgestellt und bewertet, welche für in China tätige ausländisch-investierte Unternehmen von Relevanz sind.

I. Erweiterter Anwendungsbereich

Die Novelle des Anti-Spionage-Gesetzes ergänzt in Art. 4 Abs. I zunächst die beispielhafte **Aufzählung von Spionagehandlungen**. Unverändert zur Ursprungsfassung werden Spionagehandlungen nach dem novellierten Gesetz als (1) "*Handlungen, die **die nationale Sicherheit der Volksrepublik China gefährden** […]* definiert.

Der unter Nr. (2) gelistete Tatbestand "*Beteiligung an Spionageorganisationen oder Annahme von Aufträgen von Spionageorganisationen und deren Agenten"* wurde durch **"Überlaufen zu Spionageorganisationen und deren Agenten"** *ergänzt*.

Nach Nr. (3) kann neben *"Diebstahl, Ausspähung, Bestechung oder illegalen Weitergabe von Staatsgeheimnissen, nachrichtendienstlichen Informationen […]"* neuerdings auch die **Weitergabe von *"anderen Dokumenten, Daten, Informationen oder Gegenständen, die sich auf die Sicherheit und die Interessen des Staates beziehen**, […]"*, als Spionagehandlung eingestuft werden.

Als Reaktion auf „nicht-traditionelle Sicherheitsbedrohungen" wurde die Aufzählung unter Nr. (4) durch einen neuen Tatbestand ergänzt: ***"Durchführung von Cyberangriffen, Eindringen, Einmischung, Kontrolle oder Sabotage gegen staatliche Organe, als geheim eingestufte Einheiten oder kritische Informationsinfrastrukturen usw.** […]".*

Die unter Nr. (5) aufgezählten Handlungen: *"Aufzeigen von Angriffszielen für den Feind"* und Nr. (6): "*Durchführung sonstiger Spionagetätigkeiten*" bleiben inhaltlich unverändert.

Auch Art. 4 Abs. II der Novelle erweitert den Anwendungsbereich auf "[…] ***Spionageorganisationen und ihre Agenten**, die im Hoheitsgebiet der Volksrepublik China oder unter Ausnutzung von Bürgern, Organisationen oder anderen Bedingungen der Volksrepublik China **Spionagetätigkeiten** gegen ein Drittland **durchführen und die nationale Sicherheit der Volksrepublik China gefährden**."*. Diese Ergänzung erweitert den Anwendungsbereich auf Spionagehandlungen gegen Drittländer, welche die nationale Sicherheit Chinas gefährden.

In Verbindung mit Art. 4 Abs. I Nr. (1) (vorher Art. 38 Abs. I Nr. (1)), der sich auf Spionageorganisationen, deren Agenten, die von diesen finanzierten Dritten oder Institutionen, Organisationen oder Einzelpersonen innerhalb oder außerhalb des Landes bezieht, deckt das Anti-Spionage-Gesetz nunmehr ein breiteres Spektrum von Adressaten ab, einschließlich ausländisch-investierter Unternehmen, innerhalb und außerhalb Chinas.

II. Befugnisse der Sicherheitsbehörden und Rechte der Verdächtigten

Das neue Anti-Spionage-Gesetz führt in Kapitel III neue **Prozessbestimmungen für das Ermittlungsverfahren** ein und konkretisiert die **Ermittlungsbefugnisse der nationalen Sicherheitsbehörden**.

Bei der Durchführung von Spionagebekämpfungsmaßnahmen dürfen die Behörden elektronische Geräte, Ausrüstungen, Programme und Werkzeuge der betreffenden Personen und Organisationen untersuchen und auch auf relevante Dokumente, Daten und Gegenstände zugreifen und diese beschlagnahmen oder in Verwahrung nehmen. Für die Untersuchung der vorstehenden Gegenstände müssen[1] die Behörden nun eine Genehmigung von der höheren Verwaltungsbehörde erhalten.

Weiter stellt die Novelle klar, dass die Behörden die einschlägigen Dokumente, Daten, Informationen und Gegenstände im Rahmen "des gesetzlich gestatteten Umfangs" einsehen und abrufen dürfen, und dass die betroffenen Personen dabei zur Zusammenarbeit verpflichtet sind.

Bei der Ermittlung der Spionagehandlungen sind die Behörden nach der Novelle befugt, Räumlichkeiten und Einrichtungen zu betreten bzw. Vermögensgegenstände, die für Spionagezwecke genutzt wurden, zu beschlagnahmen als auch Bankkonten einzufrieren. Die Ermittlungsmaßnahmen müssen durch mindestens zwei Personen durchgeführt werden und der Ermittlungsprozess soll auf Video aufgenommen werden. Das novellierte Gesetz legt weiterhin fest, dass bei der Durchführung der vorstehenden Maßnahmen die Behördenvertreter sich mit einem Dienstausweis ausweisen müssen.

Das Anti-Spionage-Gesetz sieht neue **Rechte der Verdächtigten im Vernehmungsprozess** vor. Die Behörden müssen[2] die betroffene Person grundsätzlich schriftlich zur Vernehmung vorladen. Eine mündliche Vorladung bei einer "auf frischer Tat ertappten" Person bzw. bei einer zwangsweisen Vorführung im Fall einer Weigerung ist jedoch gestattet. Die Behörden müssen die Familienangehörigen der vorgeladenen Person unverzüglich über die Gründe der Vorladung unterrichten, es sei denn, eine solche Unterrichtung ist "unmöglich" oder könnte die Ermittlungen behindern. Die Vernehmung darf 8 Stunden bzw. bei Straftatverdacht oder beim Verhängen einer Verwaltungshaft 24 Stunden nicht überschreiten. Dem Verhörten muss die erforderliche Zeit zum Essen, Trinken und Ausruhen gewährt werden.

Die neu hinzugefügten Befugnisse der Sicherheitsbehörden und Rechte der Verdächtigten stellen unserer Ansicht eine positive Neuerung dar, da diese die vorher nur allgemeinen behördlichen Handlungsbefugnisse konkretisieren und die Rechtsposition des Verdächtigen stärken.

III. Haftung

Im Vergleich zur ursprünglichen Fassung sieht das novellierte Anti-Spionage-Gesetz neben der Verwaltungshaft neuerdings auch Geldbußen für (Einzel-)Personen bzw. Unternehmen sowie deren Geschäftsführung vor.

Nach der Novelle können für Spionagehandlungen durch **Einzelpersonen**, welche noch keine Straftat darstellen, eine Verwaltungshaft von bis zu 10 Tagen und Geldbußen von bis zu CNY 50.000.- verhängt werden. Bei einem (durch die Spionagehandlungen erzielten) illegalen Gewinn

[1] Aufgrund des fehlenden Modalverbs in der chinesischen Sprachfassung lässt sich nicht eindeutig erschließen, ob es sich um eine "muss" oder "soll" Bestimmung handelt.

[2] Aufgrund des fehlenden Modalverbs in der chinesischen Sprachfassung lässt sich nicht eindeutig erschließen, ob es sich um eine "muss" oder "soll" Bestimmung handelt.

von mehr als CNY 50.000.- können darüber hinaus Geldbußen von bis zum Fünffachen des illegalen Gewinns verhängt werden.

Unternehmen und anderen Organisationen drohen Geldbußen von bis zu CNY 500.000.- oder bis zum Fünffachen des illegal erzielten Gewinns, wenn der illegale Gewinn mehr als CNY 500.000.- beträgt, sowie das temporäre Verbot der Geschäftstätigkeit und Entzug der Geschäftslizenz. Die **Geschäftsführung** dieser Unternehmen und Organisationen kann mit Verwaltungshaft und Geldbußen nach dem vorstehendenden Absatz bestraft werden.

Für den Fall der Verweigerung der Zusammenarbeit bei der Datenbeschaffung durch die Behörden verweist das novellierte Anti-Spionage-Gesetz nunmehr auf die Sanktionen nach dem Datensicherheitsgesetz, nach dem Geldbußen von bis zu CNY 500.000.- für Unternehmen und Geldbußen von bis zu CNY 100.000.- für die Geschäftsführung und die unmittelbar verantwortlichen Personen verhängt werden können.

Neu sind im novellierten Anti-Spionage-Gesetz Informationspflichten der Behörden, nach den die Behörden die betroffene Person vorab über den Inhalt, die Fakten, die Gründe und die Grundlage der zu verhängenden Verwaltungsstrafe sowie über deren Rechte unterrichten müssen.

Sowohl nach dem alten als auch nach dem novellierten Anti-Spionage-Gesetz können Spionagehandlungen, die eine Straftat darstellen, **strafrechtlich geahndet** werden. Nach dem Strafgesetz der VR China umfassen einschlägige Straftaten Spionage, Diebstahl, Bestechung, illegale Weitergabe von Staatsgeheimnissen oder nachrichtendienstlichen Informationen an ausländische Stellen, Untergrabung der Staatsgewalt und Finanzierung von Aktivitäten, die die nationale Sicherheit gefährden. Die vorstehenden Straftaten werden mit einer **Freiheitsstrafe von mindestens drei Jahren** bestraft.

Fraglich ist, ob die durch die Novelle neu eingeführten Geldbußen als ein milderes Sanktionsmittel betrachtet werden können, oder ob diese in der Praxis nur zusätzlich zu den bestehenden Sanktionen angewendet werden. Schlimmstenfalls führen die Geldbußen dazu, dass niederschwellige Spionagehandlungen, die vorher straffrei geblieben sind, nun mit Geldbußen belegt werden.

IV. Auswirkungen der Novelle auf (ausländisch-investierte) Unternehmen

Wie oben dargelegt, erweitert die Novelle des Anti-Spionage-Gesetzes die Aufzählung von Spionagehandlungen, konkretisiert Bestimmungen zum Ermittlungsverfahren und enthält neue Sanktionen.

Was die erweiterten Spionagehandlungen in Art. 4 betrifft, so konnten diese schon vor der Novellierung unter die bestehenden Tatbestände subsumiert werden, zumindest unter die *Catch-all-Klausel* in Art. 4 Abs. I Nr. (6) "*Durchführung sonstiger Spionagetätigkeiten"*.

Was nach wie vor unklar bleibt, ist welche Handlungen als Spionage eingestuft werden können. Im schlimmsten Fall könnten die folgenden im allgemeinen Geschäftsleben regelmäßig vorkommenden Tätigkeiten unter den Begriff der Spionage subsumiert werden:

- Sammeln von Geschäftsinformationen im Rahmen von Marktanalysen;
- Sammeln von Unternehmensinformationen im Rahmen von Due Diligence bei M&A Transaktionen;
- Grenzüberschreitende Kooperationsprojekte mit Datenaustausch/Technologietransfer;
- Einstellung von ehemaligem Regierungspersonal als Berater;
- Grenzüberschreitender akademischer/wissenschaftlicher Austausch in bestimmten Forschungsbereichen;

- Kommunikation oder Zusammenarbeit mit Unternehmen/Personen, die als Spione eingestuft werden.

In den Medien wurde über Ermittlungen der chinesischen Behörden gegen prominente Beratungsunternehmen berichtet, darunter Capvision, Bain & Company, Mintz Group und weitere Unternehmen, die "nur" Marktdaten und Finanzinformationen über chinesische Unternehmen gesammelt und deren ausländischen Kunden zur Verfügung gestellt haben. Im Rahmen bzw. infolge dieser Ermittlungen haben die chinesischen Behörden Büros, Dokumente und Daten untersucht, Mitarbeiter verhört und verhaftet und temporäre Einstellung der Geschäftstätigkeit angeordnet.

Obwohl diese Fälle oft in Verbindung mit dem Anti-Spionage-Gesetz gebracht werden, haben die Behörden in den meisten Fällen weder die Rechtsgrundlage für die behördlichen Maßnahmen und Sanktionen noch andere Einzelheiten veröffentlicht. Es ist daher zurzeit unklar, ob diese Maßnahmen auf der Grundlage des Anti-Spionage-Gesetzes oder anderer Vorschriften erfolgten. Auch fanden die meisten der Fälle noch vor dem Inkrafttreten des novellierten Anti-Spionage-Gesetzes statt.

Wir sind daher der Meinung, dass die Novelle des Anti-Spionage-Gesetzes, wenn überhaupt dann nur geringe zusätzliche Risiken mit sich bringt, da die meisten Risiken, wie oben beschrieben, bereits vor der Novelle bestanden.

Abschließend ist anzumerken, dass im Rahmen einer Gesetzesinterpretation immer auch der historische Kontext berücksichtigt werden sollte. Daher sollte auch die Novelle des Anti-Spionage-Gesetzes nicht isoliert, sondern im Kontext der chinesischen Gesetzgebung und Politik in den letzten zehn Jahren, betrachtet werden.

Bereits 2014 stellte Xi Jinping das Konzept der gesamtheitlichen Betrachtung der nationalen Sicherheit vor, nach dem die nationale Sicherheit nicht nur die politische, militärische und innere Sicherheit, sondern andere wichtige Bereiche umfassen soll, einschließlich der öffentlichen Sicherheit, Cybersicherheit und Datensicherheit. Aufgrund dieses neuen Ansatzes wurde seit 2014 neben dem Anti-Spionage-Gesetz eine Reihe von Gesetzen zum Schutz von nationalen Interessen erlassen. Diese umfassen u.a. das nationale Sicherheitsgesetz von 2015, das Cybersicherheitsgesetz von 2017 und das Datensicherheitsgesetz von 2021 und die geplante Novelle des Gesetzes zum Schutz von Staatsgeheimnissen.

Somit ist zu beachten, dass sich neben dem Anti-Spionage-Gesetz auch aus anderen Gesetzen ähnliche Risiken ergeben, da auch diese mit unbestimmten Begriffen wie "nationale Sicherheit" oder "wichtige Daten" arbeiten und strenge Sanktionen vorsehen.

V. Wie können Unternehmen Risiken reduzieren?

Hier ist keine generelle Empfehlung möglich, da jedes Unternehmen anders aufgestellt ist und damit auch die Risiken unterschiedlich sind. Es empfiehlt sich daher, mit einer Risiko-Analyse zu beginnen, um mögliche Risiken im eigenen Unternehmen zu erkennen und entsprechende Maßnahmen zur Risikoreduzierung effektiv umsetzen zu können.

Die im Unternehmen verarbeiteten Daten spielen dabei eine zentrale Rolle. Es ist deshalb u.a. zu analysieren, welche Arten von Daten im Unternehmen verarbeitet werden, wo diese gespeichert werden, wer Zugriff auf diese Daten hat, und an welche Personen die Daten weitergeleitet werden. Auf Grundlage dieses "Datenmappings" können die Daten anschließend je nach Risikoklasse kategorisiert werden, was im Hinblick auf den sehr allgemein formulierten Wortlaut des Anti-Spionage-Gesetzes für viele Unternehmen eine Herausforderung darstellen wird.

Da China komplexe und weitreichende Gesetze zum Datenschutz, Datensicherheit und Cybersicherheit hat, sollten sich Unternehmen über die Anforderungen dieser Gesetze im Klaren sein und ein solides Compliancesystem etablieren, um das Risiko von Gesetzesverstößen möglichst zu minimieren.

Neben den Maßnahmen zur Wahrung der Vertraulichkeit innerhalb des Unternehmens sollten unternehmenseigene Datensysteme auf Daten- und Cybersichersicherheit geprüft und optimiert werden, um Datenleaks zu vermeiden.

Weiter ist es empfehlenswert, einen Krisenmanagementplan zu formulieren und Mitarbeiterschulungen durchzuführen, um auf unangekündigte Ermittlungsmaßnahmen der Behörden (“dawn raids”) schnell und richtig reagieren zu können.

Sollten Sie bei der Planung und Umsetzung der vorstehenden beschriebenen Maßnahmen rechtliche Unterstützung benötigen oder Fragen hierzu haben, steht Ihnen Burkardt & Partner mit Rat und Tat gerne zur Verfügung.

Ihr Burkardt & Partner Team