жданин может непосредственно ссылаться на права, которые ясно определены и гарантированы в Директиве ЕС.

Это прежде всего касается принципиального запрета на обработку так называемой «sensitive data» «чувствительной» информации. При этом имеются в виду все сведения, касающиеся расового и этнического происхождения, политических и мировоззренческих взглядов, здоровья и сексуальной жизни. Так, например, сведения о состоянии здоровья работника не могут без его согласия быть переданы работодателю.

После сентябрьской трагедии 2001 года в США Германия предприняла ряд шагов против терроризма. В январе 2002 года вступил в силу Закон о борьбе с терроризмом, который существенно изменил действующее законодательство. Среди наиболее важных изменений – создание законодательной базы для использования биометрических данных в паспортах и карточках идентификации, упрощения механизма обмена информацией между государственными органами, предоставление секретным службам права на истребование у провайдеров, авиалиний и туристических агентств информации об их пользователях, создание базы данных образцов голоса. В феврале 2002 года Министр внутренних дел объявил, что антитеррористические меры будут включать введение биометрических ID-карточек для всех граждан страны (с использованием шифрования), а также более широкое распространение систем контроля, основанных на дактилоскопии и анализе внешности. Уже известно несколько случаев, когда граждане протестовали против этих нововведений. Германия является членом Совета Европы, подписала и ратифицировала Конвенцию о защите личности в связи с автоматической обработкой персональных данных (ETS No. 108), а позднее и дополнительный протокол к Конвенции. Германия подписала и ратифицировала Европейскую Конвенцию о защите прав человека и основных свобод, в ноябре 2002 года Германия подписала Конвенцию о киберпреступности.

KRYPTOGRAFIERECHTLICHE ASPEKTE GLOBALER UNTERNEHMENSKOMMUNIKATION

О. О. Бельская

Kryptographie (aus dem griechischen *kryptós*, «versteckt», und *gráphein*, «schreiben») ist die Wissenschaft der Verschlüsselung und Verschleierung von Informationen («Geheimschriften»). Sie ist ein Teilgebiet der Kryptologie.

Bei der Kryptografie geht es um die Idee, wichtige Informationen vor anderen Personen zu verbergen. Dabei bedient man sich der Chiffrierung, also

der Verschlüsselung. Man codiert die Informationen und gibt den Schlüssel nur an Personen weiter, welche diese Informationen lesen dürfen. Nur anhand dieses Schlüssels ist es möglich, die Codierung wieder rückgängig zu machen und so die ursprünglichen Daten zu erhalten.

Kryptographie ist als die «Lehre der Verschlüsselung von Daten» aufgrund der bestehenden Computer- und Internet-Sicherheitsprobleme so aktuell wie nie zuvor.

An moderne kryptographische Verfahren werden im wesentlichen vier Anforderungen gestellt.

Vertraulichkeit: Der Inhalt eines Dokuments soll nur von dazu befugten Personen gelesen werden können. **Integrität:** Der Inhalt eines Dokuments soll nicht unbemerkt verändert werden können. **Authentikation:** Der Urheber eines Dokuments soll feststellbar sein; kein anderer soll sich als Urheber ausgeben können. **Verbindlichkeit:** Der Urheber eines Dokuments soll seine Urheberschaft nicht abstreiten können. Ein weiteres Ziel kann in manchen Situationen **Anonymität** sein.

Um Kryptographie tatsächlich anwenden zu können, müssen sich Sender und Empfänger auf ein bestimmtes Verfahren einigen, das sie verwenden wollen.Krypto Verschlüsselungsverfahren lassen sich in drei Gruppen einteilen: *Symmetrische*, *asymmetrische* und *hybride Verschlüsselungsverfahren*.

Zur Zeit steigen die B2B-Umsätze im eBusiness kontinuierlich. So erwarten Analysten auf Grund von Studien aus Juli 2002 eine Steigerung des Onlinehandels im B2B in Europa von etwa 78 Mrd. Euro im Jahr 2001 auf über 2 Billionen Euro im Jahr 2006, was einem Anteil von 22 % des gesamten Handelsumsatz in Europa entspräche. Parallel schreitet die Integration von Daten und Sprache in global tätigen Unternehmen unter Nutzung von IP-Netzen bzw. des Internets weiter voran. Marktuntersuchungen der International Data Corporation (IDC) haben ergeben, dass im Jahre 2004 voraussichtlich 20 Prozent der europaweit agierenden Unternehmen IP-Lösungen in ihre Unternehmensnetze integriert und Virtual Private Networks (VPN) eingerichtet haben werden.

Die Gewährleistung der Sicherheit und Integrität der internationalen Unternehmenskommunikation auf der Basis modernster Systemarchitekturen und sicherer kryptografischer Verfahren steht im Zentrum der unternehmerischen Überlegungen.

Kryptografie bietet Kommunikationsteilnehmern die Möglichkeit, ihre Mitteilungen (z. B. Email) oder sonstigen Datenpakete so vertraulich zu übermitteln, dass diese von Dritten, also auch von Strafverfolgungsbehörden, nicht gelesen bzw. nur unverständlich gelesen werden können. Die moderne

Kommunikation im Computerzeitalter über weltweite öffentliche Datennetze, vorrangig das Internet, hat das Bedürfnis der Nutzer nach Vertraulichkeit verstärkt. Viele mittelständische Unternehmen aber auch Großkonzerne, die sich zur Kommunikation des Internets bedienen, richten so genannte Virtuelle Private Netzwerke (VPN) unter Verwendung von kryptografischen Verfahren ein, um ihre Mitteilungen vertraulich zu übermitteln. Es entsteht ein (virtuell) privates Netzwerk, das einem geschlossenen Benutzerkreis Dienste und Anwendungen zur Verfugung stellt, wie sonst nur das eigene Unternehmensnetz. Die Vertraulichkeit kann so in VPN: zwischen der Firmenzentrale und Zweigniederlassungen (Intranet-VPN), zwischen einem Firmennetz und mobilen Mitarbeitern (Remote-Access-VPN) und zwischen einem Unternehmen und strategischen Partnern, Kunden (Extranet VPN) gewahrt werden. Der Grad der Vertraulichkeit hängt von vielen Faktoren ab. Namentlich hängt der Grand von dem gewählten Verschlüsselungsverfahren (z. B. asymmetrische oder symmetrische Verschlüsselung), nicht zuletzt von der geählten Schlüssellänge ab. Verallgemeinert kann man sagen, dass mit zunehmender Schlüssellänge die Sicherheit einer verschlüsselten Kommunikation zunimmt.

Wie jede neue Technologie hat diese Technologie aber auch Nachteile. Kryptographie ermöglicht es Kriminellen, ihre Aktivitäten zu verbergen. Staatliche Stellen haben die Verschlüsselung immer schon als Gefahr für die Staatssicherheit gesehen. Massennutzung moderner Kommunikationswege wie Internet, die Vereinfachung der Verschlüsselung für Jedermann, sowie die Erkenntnis, dass die organisierte Kriminalität, insbesondere Terroristen verschlüsselt kommunizieren, verstärken das Bedürfnis vieler Staaten nach einer stärkeren Kontrolle.

In vielen Ländern unterliegen Hard- und Softwareimplementationen von kryptographischen Algorithmen einem Exportverbot. International werden diese Exportverbote im Wassenaar-Abkommen geregelt, das im Juli 1996 von 31 Ländern unterzeichnet wurde. Eigentliches Ziel des Abkommens ist die Kontrolle und das Transparentmachen des Transfers militärischer und sogenannter «Dual Use»-Güter – Produkte und Technologien, die sowohl für zivile als auch militärische Zwecke verwendet werden können. Unter den «Dual Use»-Gütern listet das Wassenaar-Abkommen in der Kategorie 5.2. «Informationssicherheit» auch Verschlüssellungstechnologienun Kryptosoftware, die auch als Kriegswaffe nutzen können. Daher wird Verschlüsselungstechnologie, von Land zu Land in unterschiedlichem Maße, staatlich kontrolliert.

Bei der Nutzung von Kryptosoftware/-technik und dem Transfer zwischen Staaten kommen für Kryptografie kontrollierende Gesetze grundsätzlich drei

Regelungsansätze in Betracht: die nationalen Exportvorschriften (Export Controls), die im Empfängerfand gültigen Importvorschriften (Import Controls), die jeweiligen inländischen Nutzungsvorschriften (Domestic Crypto Regulations).

Gesetzliche Regelungen sowie die Intensität der staatlichen Kontrollen unterliegen teilweise gravierender Veränderungen. Sie reichen vom gänzlichen Verbot der Nutzung von Kryptosoftware (z. B. Pakistan) Über Kompromisslösungen (z. B. Indien) bis hin zur völligen Freiheit (derzeit z. B. Brasilien).Während nationale Exportvorschriften dem Schutz vor anderen Staaten bzw. deren Bürger dienen, entspringen nationale Import- und Nutzungsvorschriften eher dem Bedürfnis nach innerer

Sicherheit der jeweiligen Staaten. Westliche Industrienationen, darunter auch Deutschland, haben sich im Wesentlichen auf Exportkontrollen beschränkt.

Nutzungsvorschriften regeln zum Teil ein gänzliches Verbot, teilweise auch verschiedenste Lösungen zur Dechiffrierung durch staatliche Stellen. Wollen staatliche Stellen die Entschlüsselung gewährleistet sehen, so regeln die Vorschriften den Zugang zur unverschlüsselten Nachricht dadurch, dass entweder vor, während oder nach der Kommunikation durch entsprechende Entschlüsselungsprogramme bzw. die Hinterlegung eines Schlüssels der Einblick in die Kommunikation ermöglicht wird.

Rechtsquelle des europäischen Ausfuhrrechts ist vor allem die Dual-Use-Verordnung Nr.1334/2000 nebst Anhängen I bis IV (nachfolgend: Dual-Use-VO), ferner das Wassenaar-Arrangement (Bestandteil der Dual-Use-VO) sowie in Deutschland das Außenwirtschaftsgesetz (AWG) und die Außenwirtschaftsverordnung (AWV), welche ergänzende Vorschriften insbesondere zum Genehmigungsverfahren enthalten. Vergleichbare Ausfuhrvorschriften enthalten die Mitgliedsstaaten der Europäischen Union. International haben viele Staaten die Exportvereinbarung zu Kryptogütern entsprechend dem Wassenaar-Abkomrnen umgesetzt. Import- und Domestic Controlls sind in Europa nur begrenzt zu finden. Zu den Importkontroll Vorschriften zählen vor allem die Total- oder Teilembargo-Resolutionen des Sicherheitsrates der Vereinten Nationen, welche durch nationale Vorschriften in verbindliches Recht umgesetzt werden müssen.

In Deutschland gilt für die Exportkontrolle nach § l des Außenwirtschaftsgesetzes (AWG) der Grundsatz der Freiheit des Außenwirtschaftsverkehrs. Allerdings sind gemäß § 7 AWG Beschränkungen möglich, um die Sicherheit der Bundesrepublik Deutschland zu gewährleisten, eine Störung des friedlichen Zusammenlebens der Völker zu verhüten oder zu verhüten, dass die auswärtigen Beziehungen der Bundesrepublik Deutschland erheblich gestört werden. Auf dieser Grundlage sind in der Außenwirtschaftsverordnung (AWV)

konkrete Verbote und Genehmigungspflichten geregelt. Die Bestimmungen ermöglichen neben der Kontrolle des Exports von Waffen und Rüstungsgütern auch die Verwaltungskontrolle über so genannte Dual-Use-Güter.

Systematisch setzt die Kontrollregelung zunächst am Exportprodukt an. In Übereinstimmung mit dem Wassenaar-Abkomrnen werden Dual-Use-Güter durch die Dual-Use-VO für alle 15 Mitgliedsstaaten einheitlich in einer Güterliste, der so genannten «Dual-Use-Liste» festgelegt, deren Ausfuhr gemäß Art. 3 I Dual-Use-VO grundsätzlich der Genehmigung bedarf. Die Dual-Use-Liste ist identisch mit Teil C der Ausfuhrliste der AWV in Deutschland. Kryptoprodukte werden dort insbesondere von Kategorie 5 Teil 2 «Informationssicherheit» und Kategorie 4 «Rechner» erfasst.

Ist Kryptosoftware von der Dual-Use-Liste nicht erfasst und besteht auch kein Handelsembargo gegen das Exportland, so kann die Software unproblematisch auch in ein außereuropäisches Land exportiert werden. So ist der Export von Kryptosoftware, welche z. B. auf dem privaten Notebook bei Auslandsreisen mitgefiihrt wird, nicht genehmigungspflichtig.

Bereits nach der Kryptotechnik-Anmerkung zur Dual-Use-Liste Teil 2 - Informationssicherheit unterlagen im Ausfuhrland frei erhältliche Kryptoprodukte unter bestimmten Voraussetzungen keiner Ausfuhrkontrolle. Mit VO 428/2001 EG vom 6.3.2001 ist nunmehr auch der Export von Software von der Ausfuhrkontrolle ausgenommen, wenn diese frei erhältlich ist und im Einzelhandel im Bar-oder Versandverkauf, per Download oder Telefon vertrieben wird, zudem nicht leicht verändert sowie leicht installiert werden kann.

Soweit der Export von Kryptoprodukten aus einem Mitgliedsland der EU Produkt bezogen genehmigungspflichtig ist, kommen drei Formen der Genehmigung, die Allgemeingenehmigung (AG), die Sammelgenehmigung oder die Einzelgenehmigung in Betracht.

In Deutschland gilt für Güter der Telekommunikation und Informationssicherheit darüber hinaus die AG Nr. 16 vom l \.9.2000, welche den Export von Kryptoprodukten einschließlich Informationssicherheit allgemein in alle Länder genehmigt, es sei denn, dass sie bereits von der EU001 wegen ihres Vorrangs erfasst werden oder dass die Länder Ausfuhrbeschränkungen unterliegen (Embargoländer).

Zusammenfassend lässt sich feststellen: Der Export von Kryptosoftware ist, soweit nach der Dual-Use-Liste genehmigungspflichtig, EU-weit für viele Länder allgemein genehmigt. In Deutschland besteht darüber hinaus eine allgemeine Genehmigung in Form der AG Nr. 10 und AG Nr. 16 für fast alle Länder, die keiner sonstigen Ausfuhrbeschränkung unterfallen. Der Import von Kryptosoftwäre wird in Mitgliedsländern der EU durch allgemeine Embargoregelungen eingeschränkt.

Das Internet ist unsicher! Jegliche ungeschützte Kommunikation kann abgehört und die daraus gewonnenen Informationen missbraucht werden. Davor kann man sich mit Kryptographie zuverlässig schützen.

Für Unternehmen gilt es im Kryptographierecht die in Frage kommenden staatlichen Kontrollregelungen, das Prozedere eines ggf. erforderlichen Genehmigungsverfahrens und die möglichen Folgen der Nichtbeachtung staatlicher Kryptoregelungen zu kennen. Eine rechtssichere Abklärung kryptografierechtlicher Fragen erfordert daher immer eine 3-fach Prüfung vor Einrichtung kryptografischer Verfahren in der globalen Unternehmenskommunikation.

ПОЛИТИКА КНР В ЦЕНТРАЛЬНОЙ АЗИИ И ВОЗНИКНОВЕНИЕ ШАНХАЙСКОЙ ОРГАНИЗАЦИИ СОТРУДНИЧЕСТВА

В. Р. Боровой

Распад СССР вызвал глубокие изменения в системе международных отношений, в том числе и в Центральной Азии. Среди основных особенностей ситуации в данном регионе в 90-е гг. XX в. можно назвать следующие.

Светские режимы стран Центральной Азии в ряде случаев столкнулись с серьезной внутренней нестабильностью, связанной с этническими и религиозными факторами, что вынудило их искать поддержку вовне, и способствовало проникновению в регион внешних сил.

Стремление местных режимов преодолеть естественную географическую изолированность региона и зависимость от России, прежде всего, в смысле транспортных коммуникаций, также вело к поиску новых партнеров.

Все это, а также сравнительная слабость местных государств и ограниченные возможности России привело к возникновению здесь вакуума влияния, который в меру своих возможностей и интересов попытались заполнить различные страны.

Что касается целей, которые преследовали новые игроки на центральноазиатской арене, то их можно обобщить в виде трех сценариев возможного развития региона. Во-первых, создание нового Шелкового пути, т. е. всестороннее освоение ресурсов региона и его включение в мировую экономику. Во-вторых, возникновение новой «великой игры», т. е. развитие борьбы за сферы влияние между наиболее влиятельными региональными игроками. В-третьих, вариант «мягкого подбрюшья»,