Aufsätze

Matthias Söhner

Insiderhandel und Marktmanipulation durch Geheimdienste – Informationen in Zeiten von PRISM und ihre Nutzung

I. Einleitung

Die britische Zeitung *The Guardian* hat Mitte des Jahres 2013 als streng geheim klassifiziertes Material der NSA aus den Überwachungsprogrammen *PRISM* und *Boundless Informant* veröffentlicht. Über Letzteres seien allein in einem Monat etwa 97 Mrd. einzelne Telekommunikationsdaten (Metadaten) gesammelt worden.[1] *PRISM* erlaube es darüber hinaus auch, auf den Inhalt von E-Mails, Dateien, Chats sowie Suchverläufe zuzugreifen.[2] Entsprechende Überwachungen betreibe der britische Dienst GCHQ unter dem Namen *Tempora*, wobei ein Zugriff auf transatlantische Fiberglaskabel erfolge.[3] Neben einem Informationsaustausch zwischen den USA, dem Vereinigten Königreich, Kanada, Australien und Neuseeland (sog. *Five Eyes*) bestünde dabei auch eine Zusammenarbeit mit Deutschland. Die Informationen gehen auf ein Whistleblowing *Edward Snowdens* Ende Mai 2013 zu seiner Arbeit für einen sog. *defence contractor* der NSA zurück.[4] Am 16.12.2013 erging eine Entscheidung des *United States District Court* in Washington, die der US-Regierung das Sammeln von Metadaten der Verfahrenskläger aufgrund verfassungsrechtlicher Bedenken verbietet.[5] Derzeit beginnt in München die Produktion eines Films über *Snowden*, bei der *Oliver Stone* Regie führt.

Eine im Jahr 2011 veröffentlichte Studie der Ökonomen *Arindrajit Dube*, *Ethan Kaplan* und *Suresh Naidu* untersucht die Auswirkungen verdeckter Operationen von Ge-

1 The Guardian vom 11. Juni 2013 (abrufbar unter: http://www.guardian.co.uk/world/2013/jun/08/nsa-boundless-informant-global-datamining; letzter Abruf: 13.11.2014).

2 The Guardian vom 11. Juni 2013 (abrufbar unter: http://www.guardian.co.uk/world/2013/jun/06/us-tech-giants-nsa-data; letzter Abruf: 13.11.2014); danach sei das Überwachungsprogramm laut NSA-Angaben "one of the most valuable, unique and productive accesses for NSA".

3 The Guardian vom 21. Juni 2013 (abrufbar unter: http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa; letzter Abruf: 13.11.2014).

4 The Guardian vom 10. Juni 2013 (abrufbar unter: http://www.guardian.co.uk/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance; letzter Abruf: 13.11.2014). Zur Haftung und zu den Rechten US-amerikanischer whistleblower s. bereits Vladeck, 57 American University L. Rev. (2008), 1531 ff.

5 Klayman et al. v. Obama et al. (13-0851)(nrk)(abrufbar unter: https://ecf.dcd.uscourts.gov/cgi-bin/show_public_doc?2013cv 0851-48; letzter Abruf: 13.11.2014). Über das von der US-Regierung eingelegte Rechtsmittel ist noch nicht entschieden.

10.5771/0023-4834-2015-1-56

heimdiensten auf die Börsenkurse betroffener Unternehmen. Danach war in einem Zeitraum von 16 Tagen vom Zeitpunkt des Beschlusses der Operation an ein Kursanstieg um durchschnittlich 13% zu verzeichnen.[6] Dies legt nahe, dass es im Vorfeld der Ausführung zu undichten Stellen kam. Dabei wirken sich nicht nur Putschversuche auf den Börsenkurs solcher Unternehmen aus, bei denen zuvor Vermögenswerte von der missliebigen Regierung verstaatlicht wurden. Denkbar kursrelevant sind auch andere Informationen, die durch Wirtschaftsspionage[7] oder zufällig gewonnen werden, wie betreffend technisches Know-how, Fertigungstechniken, wirtschaftspolitische Strategien, sozialökonomische und politische Trends, Unternehmens-, Markt- und Absatzstrategien, Zielrichtungen und Methoden der Forschung, Wettbewerbsstrategien, Preisgestaltung und Konditionen sowie Zusammenschlüsse und Absprachen von Unternehmen.[8] Dies gilt freilich auch für Ad-hoc-Informationen wie wichtige Vertragsabschlüsse, Ölfunde, Produktfehler, Gewinnschätzungen oder bevorstehende Übernahmeangebote.

Insoweit drängt sich die Frage auf, inwieweit über eine Strafbarkeit wegen Geheimnisverletzung hinaus Mitarbeiter von Geheimdiensten, die schon von Berufs wegen über einen – in Zeiten von *PRISM* und *Tempora* wohl beträchtlichen – Informationsvorsprung verfügen, auch gegen das Verbot von Insidergeschäften und das Verbot der Marktmanipulation verstoßen können. Dies soll im Folgenden anhand der zuvor genannten Informationen geprüft werden.

II. Geheimdienste und Geheimdienstoperationen

1. Deutschland

Auf Bundesebene[9] bestehen drei Nachrichtendienste: Hervorgegangen aus der sog. Organisation Gehlen, nahm im Jahr 1956 der Bundesnachrichtendienst (BND) als Auslandsnachrichtendienst offiziell seine Tätigkeit auf. Als Inlandsnachrichtendienst fungieren das Bundesamt für Verfassungsschutz und der dem Bundesministerium der Verteidigung zugehörige Militärische Abschirmdienst (MAD). Aufgabe des BND ist es, zur Gewinnung von Erkenntnissen über das Ausland, die von außen- und sicherheitspolitischer Bedeutung für die BRD sind, erforderliche Informationen zu sammeln und auszuwerten (§ 1 Abs. 2 BNDG); polizeiliche Befugnisse oder Weisungsbefugnisse stehen ihm dabei nicht zu (§ 2 Abs. 3 BNDG). Entsprechende Befugnisse und Grenzen gelten auch für die anderen Nachrichtendienste. Danach gewonnene geheimhaltungsbedürftige Tatsachen

6 Dube/Kaplan/Naidu, Coups, Corporations and Classified Information, 126 The Quarterly Journal of Economics (2011), 1375 ff.

7 Bundesamt für Verfassungsschutz für die Verfassungsschutzbehörden des Bundes und der Länder, Wirtschaftsspionage: Risiko für Unternehmen, Wissenschaft und Forschung, Juli 2014 (abrufbar unter: http://www.verfassungsschutz.de/embed/broschuere-2014-07-wirtschaftsspionage.pdf; letzter Abruf: 13.11.2014): neben der politischen und militärischen Ausforschung ein klassisches Aufklärungsziel von Geheimdiensten. Überschreiten konkurrierende Unternehmen bei ihren Umfeld-, Konkurrenz-und Produktanalysen die vom UWG gezogenen Grenzen, spricht man indes von Konkurrenzausspähung oder Industriespionage.

8 Bundesamt für Verfassungsschutz (Fn. 7), S. 7.

9 Auf Landesebene sind ebenfalls Verfassungsschutzbehörden eingerichtet. Nachrichtendienstliche Aufgaben werden ferner vom Bundesamt für Sicherheit in der Informationstechnik sowie dem IKTZ der Bundespolizei wahrgenommen.

werden entsprechend ihrer Schutzbedürftigkeit in die Geheimhaltungsgrade „STRENG GEHEIM“, „GEHEIM“, „VS-VERTRAULICH“ oder „VS-NUR FÜR DEN DIENSTGEBRAUCH“ eingestuft.[10] Die Nachrichtendienste sind ferner zur Telekommunikationsüberwachung und -aufzeichnung nach dem Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz – G 10) berechtigt.[11]

Nach dessen § 1 Abs. 1 kann sie zur Abwehr von drohenden Gefahren für die freiheitliche demokratische Grundordnung oder den Bestand oder die Sicherheit des Bundes oder eines Landes einschließlich der Sicherheit der in der BRD stationierten Truppen der nichtdeutschen Vertragsstaaten des Nordatlantikvertrages erfolgen. Der BND darf dies im Rahmen seiner Aufgaben nach § 1 Abs. 2 BNDG auch zu den in § 1 Abs. 1 Nr. 2, § 5 Abs. 1 Satz 3 Nr. 2 bis 7 und § 8 Abs. 1 Satz 1 G 10 bestimmten Zwecken. Beschränkungen nach § 1 Abs. 1 Nr. 1 G 10 dürfen angeordnet werden, wenn tatsächliche Anhaltspunkte für den Verdacht bestehen, dass eine Katalogtat des § 3 Abs. 1 oder Abs. 1a G 10 (bspw. Hochverrat, Gefährdung des demokratischen Rechtsstaats oder der äußeren Sicherheit) geplant wird oder begangen wurde. Beschränkungen nach § 1 G 10 für internationale Telekommunikationsbeziehungen, soweit eine gebündelte Übertragung erfolgt (strategische Beschränkungen), sind nach § 5 Abs. 1 Satz 3 G 10 nur zulässig zur Sammlung von Informationen über Sachverhalte, deren Kenntnis notwendig ist, um u.a. die Gefahr eines bewaffneten Angriffs auf die BRD oder der Begehung internationaler terroristischer Anschläge mit unmittelbarem Bezug zur BRD rechtzeitig zu erkennen und einer solchen Gefahr zu begegnen.[12] Insoweit ist daher eine flächendeckende Überwachung durch den BND mit Suchbegriffen möglich. Anbieter von Post- und Telekommunikationsdiensten haben dabei auf Anordnung Auskunft über die näheren Umstände des Postverkehrs und der nach Wirksamwerden der Anordnung durchgeführten Telekommunikation zu erteilen sowie Sendungen, die ihm zum Einsammeln, Weiterleiten, Ausliefern und zur Übermittlung auf dem Telekommunikationsweg anvertraut sind, auszuhändigen (§ 2 Abs. 1 G 10). Danach ist ferner die Überwachung und Aufzeichnung der Telekommunikation zu ermöglichen.

Gegen entsprechende Anordnungen und deren Vollzug ist der Rechtsweg vor der Mitteilung an den Betroffenen nicht zulässig (§ 13 G 10). Anstelle dessen bedarf es nach § 14 Abs. 1 G 10 der Unterrichtung des aus einer kleinen Zahl Abgeordneter bestehenden Parlamentarischen Kontrollgremiums des Bundestags in Abständen von höchstens sechs Monaten. Von Amts wegen oder auf Grund von Beschwerden entscheidet nach geheimer Beratung ferner die vom Parlamentarischen Kontrollgremium bestellte sog. G 10-Kommission über die Zulässigkeit und Notwendigkeit von Beschränkungsmaßnahmen (§ 15

10 S. §§ 1, 2 Abs. 1, 3 Verschlusssachen-Anweisung – VSA (Allgemeine Verwaltungsvorschrift des Bundesministeriums des Innern zum materiellen und organisatorischen Schutz von Verschlusssachen vom 31. März 2006) i. V. mit § 1 Abs. 1 BNDG, § 2 Abs. 1 BVerfSchG, § 1 Abs. 1 MADG (Geltung auf Bundesebene).

11 Präventiv kann dies daneben auch aufgrund landesrechtlicher Sicherheits- und Ordnungsgesetze (wie etwa § 33a NSOG) oder §§ 23a ff. Zollfahndungsdienstgesetz bzw. repressiv aufgrund § 100a StPO erfolgen.

12 Verfassungsgemäß (BVerwG, Urt. v. 23.1.2008 – 6 A 1.07, BVerwGE 130, 180 ff.; s. auch Urt. v. 20.5.2009 – 6 A 4/08 [abrufbar unter: http://www.bverwg.de/entscheidungen/entscheidung.php?ent=200509U6A4.08.0; letzter Abruf: 13.11.2014]: eingeschränkte Überprüfbarkeit des Urteils der G 10-Kommission).

Abs. 5 G 10). Damit ist ein effektiver Rechtsschutz gegen nachrichtendienstliche Lauschangriffe faktisch ausgeschlossen.

2. USA

In den USA arbeitet eine Vielzahl von Geheimdiensten. Herausgegriffen seien hier die *National Security Agency* (NSA), die auch das Echelon-Spionagenetz betreibt, und der 1947 gegründete Auslandsnachrichtendienst *Central Intelligence Agency* (CIA). Über das reine Sammeln und Auswerten von Informationen[13] hinaus obliegt es der CIA nach § 104A(d)(4) *National Security Act of 1947* auch „andere informationsbezogene Aufgaben" auf Weisung des US-Präsidenten hin auszuführen.[14] Danach bestehen freilich weitreichende Möglichkeiten. Die Vorschrift wurde als Ermächtigungsgrundlage für geheime Operationen im Ausland angesehen.[15] Nicht geheim geblieben sind davon u.a.:

- der Sturz der Mossadegh-Regierung im Iran zusammen mit dem britischen MI6 (Project Ajax – 1953),
- der Sturz von Präsident Jacobo Árbenz Guzmán in Guatemala (Project PB/Fortune, PB/Success – 1952-1954),
- die fehlgeschlagene Invasion in der kubanischen Schweinebucht (Project Zapata – 1960-1961),
- verdeckte Operationen zur Unterminierung der Allende-Regierung in Chile (Project FU/Belt – 1970-1973),
- die Unterstützung der „Contras" in Nicaragua durch Waffenverkäufe an den Iran und die Duldung des Kokain-Schmuggels in die USA (Iran-Contra-Affäre) und
- die Erbeutung eines Großteils der Klarnamen der DDR-Agenten im Ausland nach der deutschen Wiedervereinigung (Operation Rosewood).

Belege für eine systematische Wirtschaftsspionage westlicher Geheimdienste liegen den deutschen Verfassungsschutzbehörden offiziell indes nicht vor.[16] Die elektronische- ein-

13 Entsprechend den deutschen Geheimhaltungsgraden werden in den USA (und dem Vereinigten Königreich) die Abstufungen top secret, secret, confidential und restricted verwendet (classified information).

14 50 U.S.C. § 403–4a.

15 Dazu und zu den folgenden Beispielen Dube/Kaplan/Naidu (Fn. 6), S. 1378 ff.

16 Bundesamt für Verfassungsschutz (Fn. 7), S. 13 (anders als etwa bei chinesischen und russischen Geheimdiensten); zu einem anderen Ergebnis kommt der nichtlegislative Bericht des Echelon-Ausschusses des Europäischen Parlaments vom 5.9.2001 (abrufbar unter: http://www.europarl.europa.eu/sides/getDoc.do?type=PRESS&reference=DN-20010905-1&format=XML&language=DE#SECTION1; letzter Abruf: 13.11.2014): „Der Echelon-Ausschuss stellt fest, dass es keinen Zweifel mehr an der Existenz eines globalen Kommunikationsabhörsystems geben kann, das von den USA, Großbritannien, Australien, Neuseeland und Kanada betrieben wird. Auch über die Zielsetzung des Systems, private und kommerzielle – und nicht-militärische – Kommunikation abzuhören, ist man sich einig." „Der Ausschuss appelliert an Deutschland und Großbritannien, ein weiteres Abhören der Kommunikation durch US-Geheimdienste auf ihrem Staatsgebiet an bestimmte Voraussetzungen zu binden: Ein Abhören muss in Übereinstimmung mit der Europäischen Charta für Menschenrechte des Europarates stattfinden, d. h. dass beispielsweise die Konsequenzen für Individuen vorhersehbar sein müssen.".

schließlich der Telekommunikationsüberwachung (*electronic surveillance*) wird durch den *Foreign Intelligence Surveillance Act of 1978* (FISA)[17] geregelt.

Dafür bedarf es grundsätzlich einer gerichtlichen Anordnung (*court order*)[18] eines geheim tagenden Sondergerichts, dem *Foreign Intelligence Surveillance Court* (FISC).[19] Ausreichend ist dafür, dass die Maßnahme von einem Bundesbeamten mit Zustimmung des *Attorney Generals* beantragt wurde, ein wahrscheinlicher Grund zur Annahme (*probable cause to believe*) besteht, dass das Ziel der Überwachung eine ausländische Macht (*foreign power*) oder ein Agent einer solchen ist,[20] dass die Verhältnismäßigkeit der Maßnahme (*minimization procedures*) gewahrt ist und die erforderlichen gesetzlichen Erklärungen abgegeben wurden.[21] Ein *court of review* überprüft die *Ablehnung* des Antrags.[22] Unter bestimmten Voraussetzungen kann der US-Präsident durch den *Attorney General* indes auch eine Überwachung für einen Zeitraum von bis zu einem Jahr ohne *court order* anordnen (*warrantless surveillance*).[23] In jedem Fall muss die Maßnahme zu dem Zweck erfolgen, *foreign intelligence information*[24] zu erlangen. Anbieter von Post- und Telekommunikationsdiensten (*communication common carrier*) haben dabei jeweils auf Anordnung Unterstützung zu leisten. Die Geheimdienste erhalten insoweit Informationen von Servern US-amerikanischer Internet-Unternehmen wie Google, Facebook, Apple, Microsoft und Yahoo sowie die Verbindungsdaten von Telefongesellschaften. Auch nach FISA bedarf es der Unterrichtung über entsprechende Maßnahmen an die Legislative (Kongress).[25]

Wesentlich erweitert[26] wurde das Gesetz infolge der Anschläge am 11. September 2001 mit dem sog. *Patriot Act*.[27] Weitere Kompetenzen folgten durch den *Protect America Act of 2007*[28] nach Befürchtungen des *Director of National Intelligence* (DNI) einer "*heigh-*

17 50 U.S.C. §§ 1801 ff.; allgemein dazu und zu dem "Lawless State" davor Swire, 72 Geo. Wash. L. Rev. (2004) 1306 ff. und 1315 ff.; Kris, 17 Stanford L. & Pol'y Rev. (2006) 487 ff.; Anzaldi/Gannon, 88 Texas L. Rev. (2010) 1599, 1605 ff.; kritisch (unzeitgemäß) Kerr, 75 University of Chicago L. Rev. (2008) 225 ff.

18 50 U.S.C. §§ 1802(b), 1804, 1805. In Notfällen kann sie aber nach § 1805(e) auch bis zu sieben Tage nach der Anordnung durch den Attorney General (post-hoc) beantragt werden (emergency order).

19 50 U.S.C. § 1803: "The Chief Justice of the United States shall publicly designate 11 district court judges from at least seven of the United States judicial circuits of whom no fewer than 3 shall reside within 20 miles of the District of Columbia who shall constitute a court which shall have jurisdiction to hear applications for and grant orders approving electronic surveillance anywhere within the United States under the procedures set forth in this chapter [...]" (a)(1).

20 50 U.S.C. § 1805(a)(2). Dabei herrscht ein weiteres Verständnis als das traditionelle strafrechtliche, vgl. S. Rep. No. 95-701 (1978), p. 12: "The international character of foreign terrorist activities fully supports the more flexible probable cause standard [...]".

21 50 U.S.C. § 1805(a)(4), etwa "that a significant purpose of the surveillance is to obtain foreign intelligence information" (der urspr. Wortlaut "purpose" wurde mit dem Patriot Act geändert) sowie "that such information cannot reasonably be obtained by normal investigative techniques" (§ 1804(a)(6)(B) sowie (C)).

22 50 U.S.C. § 1803(b).

23 50 U.S.C. § 1802(a). In „Kriegszeiten" greift zusätzlich § 1811.

24 50 U.S.C. § 1801(e): u.a. bzgl. den Schutz d. USA gegen Angriffe und internationale terroristische Anschläge.

25 50 U.S.C. §§ 1807 f.

26 Dazu Swire, 72 Geo. Wash. L. Rev. (2004) 1306, 1330 ff.; s. aber Wong, 43 Harvard J. on Legis. (2006), 517, 529: "largely technical amendments"; s. auch oben Fn. 21 .

27 Pub. L. No. 107-56, 115 Stat. 272 (2001).

28 Pub. L. No. 110-55, 121 Stat. 552 (2007); dazu Anzaldi/Gannon, 88 Texas L. Rev. (2010) 1599 ff.

tened terrorist threat environment" und dessen Forderung, FISAs *"requirement of a court order to collect foreign intelligence about foreign targets located overseas"* zu streichen[29] – ebenfalls unter Präsident *George W. Bush*. Danach wurde in Abgrenzung zum Begriff *electronic surveillance* eine weitere Form der *warrantless surveillance* (*directed at a person reasonably believed to be located outside of the United States*) geschaffen. Sie konnte vom DNI und *Attorney General* für einen Zeitraum von bis zu einem Jahr angeordnet werden.[30] Zwar lief diese *sunset legislation* 180 Tage nach ihrem Inkrafttreten wieder aus; für bestehende Anordnungen – die zudem unbeschränkt erneuert werden können (!) – gilt sie aber über den *FISA Amendments Act of 2008* fort,[31] mit dem zudem wieder ähnliche (aber ausdrücklich beschränkt auf Personen, die sich nicht in den USA aufhalten) detaillierte Bestimmungen[32] erlassen wurden. Im Jahr 2012 unter Präsident *Obama* verlängert, gelten diese Vorschriften bis zum 31.12.2017 fort. Das Washingtoner *United States District Court* verbot der US-Regierung indes in einer Entscheidung vom 16. Dezember 2013, weiter Metadaten der Verfahrenskläger über eine *warrantless surveillance* zu sammeln.[33] Bundesrichter *Richard J. Leon* begründet dies mit einem wahrscheinlichen (*substantial likelihood*) Verstoß gegen den vierten Zusatzartikel der US-Verfassung.[34] Die Entscheidung ist noch nicht rechtskräftig; von ihr gehen noch keine Rechtswirkungen aus.[35]

3. Vereinigtes Königreich

Im Vereinigten Königreich arbeitet der Auslandsgeheimdienst *Secret Intelligence Service* (SIS), besser bekannt unter *Military Intelligence, Section 6* (MI6) oder *Secret Service*. Ausweislich des *Intelligence Services Act 1994* kann auch der MI6 über das Sammeln und Auswerten von Informationen hinaus entsprechend „andere Aufgaben" ausführen.[36] Als Inlandsgeheimdienst fungiert der *Security Service* (MI5). Bislang eher weniger bekannt ist das *Government Communications Headquarters* (GCHQ), das neben der Kryptographie auch für die Kommunikationsüberwachung zuständig ist. Sie wird mit dem *Regulation of Investigatory Powers Act 2000* (RIPA) geregelt.

Das Gesetz hat einen außerordentlich weiten Anwendungsbereich. Auch Kommunalbehörden (*local authorities*) ermächtigend, wurde im Jahr 2008 bekannt, dass in Dorset drei Kinder und ihre Eltern wegen des Verdachts überwacht wurden, sich einen Platz in

29 S. Rep. No. 110-209 (2007), p. 5.
30 50 U.S.C. §§ 1805a-c (repealed); s. In re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1012 (FISA Ct. Rev. 2008)(vereinbar mit U.S. Constitution, Amendment 4).
31 Pub. L. No. 110–261, 122 Stat. 2436 (2008)[§ 404(a)2(A)(B),7(B)].
32 50 U.S.C. §§ 1881 ff.; jüngst bestätigt vom U.S. Supreme Court in Clapper, DNI, et al. v. Amnesty International USA et al. (11-1025)(abrufbar unter: http://www.supremecourt.gov/opinions/12pdf/11-1025_ihdj.pdf; letzter Abruf: 13.11.2014).
33 Klayman et al. v. Obama et al., S. 67 (Fn. 5).
34 Klayman et al. v. Obama et al., S. 62 (Fn. 5).
35 Klayman et al. v. Obama et al., S. 67 (Fn. 5): "However, in light of the significant national security interests at stake in this case and the novelty of the constitutional issues, I [Bundesrichter Richard J. Leon] will stay my order pending appeal.".
36 Section 1(1)(b): "to perform other tasks".

einer begehrten Schule erschlichen zu haben.[37] Ob dieses und anderer Beispiele sah sich der Vorsitzende der nationalen *Local Government Association* veranlasst, die Verantwortlichen anzuhalten, keine Überwachungen "for trivial matters" durchzuführen.[38] Post- und Telekommunikation kann mit und ohne Anordnung (*warrant*) des *Secretary of State* abgefangen werden (*interception*).[39] Ein *interception warrant* kann etwa vom *Chief* des MI6 oder dem *Director* des GCHQ beantragt werden.[40] Er muss nicht notwendigerweise eine bestimmte zu überwachende Person nennen, solange die abzufangende Telekommunikation außerhalb der *British Islands* abgesendet oder empfangen wird (*external communication*).[41] Anbieter von Post- und Telekommunikationsdiensten (*postal or telecommunications operator*) haben jeweils auf einen Bescheid (*notice*) hin Kommunikationsdaten (*communications data*) herauszugeben.[42] Die Abfangmaßnahmen unterliegen der Aufsicht eines vom Premierminister eingesetzten *Interception of Communications Commissioner* sowie einer Ex-post-Kontrolle eines Tribunals.[43] Die britische Zeitung *The Guardian* zitiert dazu einen *senior legal advisor* des GCHQ mit den Worten "We have a light oversight regime compared with the US" und das Tribunal habe "so far always found in our favour".[44] Die Verfassung des Vereinigten Königreichs ist eine Kombination aus Gesetzen, common law und ungeschriebenen Konventionen.[45] Ein Grundrechtsschutz besteht lediglich über die mit dem *Human Rights Act 1998* national durchsetzbare Europäische Menschenrechtskonvention.

III. Verbot von Insidergeschäften

§ 14 Abs. 1 Nr. 1 und 2 WpHG verbietet es, unter Verwendung einer Insiderinformation Insiderpapiere für eigene oder fremde Rechnung oder für einen anderen zu erwerben oder zu veräußern sowie einem anderen eine Insiderinformation unbefugt mitzuteilen

37 BBC News (abrufbar unter: http://news.bbc.co.uk/1/hi/england/dorset/7343445.stm; letzter Abruf: 13.11.2014).

38 LGA-Pressemitteilung vom 23. Juni 2008 (abrufbar unter: http://www.lacors.gov.uk/lacors/NewsArticleDetails.aspx?id=19649; letzter Abruf: 13.11.2014).

39 Sections 3, 4, 5, 81(1) RIPA. Section 4(1)(a) RIPA bestimmt: "Conduct […] is authorised by this section if [...] for the purpose of obtaining information about the communications of a person who, or who the interceptor has reasonable grounds for believing, is in a country or territory outside the United Kingdom". "a warrant is necessary (a) in the interests of national security; (b) for the purpose of preventing or detecting serious crime; (c) for the purpose of safeguarding the economic well-being of the United Kingdom" oder bei einem vergleichbaren Sachverhalt aus Gründen internationaler Zusammenarbeit (Section 5(3) RIPA). Section 5(5) RIPA: "A warrant shall not be considered necessary on the ground falling within subsection (3)(c) unless the information which it is thought necessary to obtain is information relating to the acts or intentions of persons outside the British Islands."

40 Section 6(2) RIPA.

41 Sections 8(4),(5), 20 RIPA: "a communication sent or received outside the British Islands". Dabei ist aber zu beachten, dass – technisch bedingt – auch eine Kommunikation zwischen Inländern über die Staatsgrenze hinweg erfolgen kann.

42 Section 22(4) RIPA.

43 Sections 57 sowie 65 ff. RIPA.

44 The Guardian vom 21. Juni 2013 (abrufbar unter: http://www.theguardian.com/uk/2013/jun/21/legal-loopholes-gchq-spy-world; letzter Abruf: 13.11.2014).

45 Insoweit ist die mitunter anzutreffende Behauptung, es bestünde keine geschriebene Verfassung, unscharf.

oder zugänglich zu machen. Fraglich ist, inwieweit ein Geheimdienstmitarbeiter dagegen verstößt, wenn er selbst entsprechende Geschäfte aufgrund geheimer Informationen tätigt oder solche Dritten preisgibt. Zentrales Tatbestandsmerkmal ist danach der Begriff Insiderinformation.

1. Insiderinformation

Nach der Legaldefinition in § 13 Abs. 1 Satz 1 WpHG ist eine Insiderinformation eine konkrete Information über nicht öffentlich bekannte Umstände, die sich auf einen oder mehrere Emittenten von Insiderpapieren oder auf die Insiderpapiere selbst beziehen und die geeignet sind, im Fall ihres öffentlichen Bekanntwerdens den Börsen- oder Marktpreis der Insiderpapiere erheblich zu beeinflussen.[46] Dabei versteht es sich freilich von selbst, dass (etwa nach der VSA)[47] geheim(haltungsbedürftig)e Informationen nicht öffentlich bekannt sind.

a) Konkrete Information über Umstände

Eine konkrete Information über Umstände stellt zunächst eine Information über Tatsachen dar.[48] Erfasst sind daher neben Informationen betreffend Putschversuche (und andere unternehmensexterne Sachverhalte [s. dazu unten b)]) auch solche bezüglich technischen Know-hows, Fertigungstechniken, wirtschaftspolitische Strategien, sozialökonomische und politische Trends, Unternehmens-, Markt- und Absatzstrategien, Zielrichtungen und Methoden der Forschung, Wettbewerbsstrategien, Preisgestaltung und Konditionen sowie Zusammenschlüsse und Absprachen von Unternehmen. Dass Geheimdienste über solche Informationen verfügen, ist „kein Geheimnis".[49] Und soweit nicht wie etwa im Vereinigten Königreich ausdrücklich auch nationale wirtschaftliche Interessen beim Abfangen der Kommunikation eine Rolle spielen ("interception [...] for the purpose of safeguarding the economic well-being of the United Kingdom"),[50] so kommen entsprechende Informationen doch jedenfalls als „Beifang" nahezu unbegrenzt verfügbarer Datenvolumina infolge von Überwachungsprogrammen wie *PRISM*, *Boundless Informant* oder *Tempora* mit in Betracht. Hinzu kommt freilich die offene Informationsbeschaffung etwa mittels dem sog. *social engineering*.[51] Konkrete Informationen sind

46 Art. 1 Nr. 1 Satz 1 der Richtlinie 2003/6/EG des europäischen Parlaments und des Rates vom 28. Januar 2003 über Insider-Geschäfte und Marktmanipulation (Marktmissbrauch) (Marktmissbrauchsrichtlinie; ABl. EU L 96 v. 12. 4. 2003 S. 16 ff.) bestimmt eine Insiderinformation als eine nicht öffentlich bekannte präzise Information, die direkt oder indirekt einen oder mehrere Emittenten von Finanzinstrumenten oder ein oder mehrere Finanzinstrumente betrifft und die, wenn sie öffentlich bekannt würde, geeignet wäre, den Kurs dieser Finanzinstrumente erheblich zu beeinflussen.

47 Siehe bereits oben II.1. mit Fn. 10.

48 Siehe nur Schwark/Kruse, in: Schwark/Zimmer, Kapitalmarktrechtskommentar, 4. Aufl., 2010, § 13 WpHG Rn. 8.

49 Bundesamt für Verfassungsschutz (Fn. 7), S. 7; Dube/Kaplan/Naidu (Fn. 6).

50 Siehe bereits oben II.3. mit Fn. 39 (section 5(3)(c) RIPA).

51 Bundesamt für Verfassungsschutz (Fn. 7), S. 28: Dabei handelt es sich um eine „Methode, um unberechtigten Zugang zu sensiblen Informationen durch ‚Aushorchen' von Personen zu erlangen. Ausgenutzt werden menschliche Eigenschaften wie […] Vertrauen, Eitelkeit, Hilfsbereitschaft, Habgier, Angst oder Respekt vor Autorität."

freilich auch Ad-hoc-Informationen betreffend wichtige Vertragsabschlüsse, Erfindungen und Entdeckungen (z.B. Ölfunde) eines Unternehmens, Produktfehler, Gewinnschätzungen oder bevorstehende Übernahmeangebote. Tatsache kann aber auch die *Äußerung* einer subjektiven Wertung sein, wie etwa die Einschätzung der Ertragslage eines Unternehmens, nicht aber die subjektive Wertung an sich.[52] Eine relevante Information kann daher auch die kundgegebene Bewertung bestimmter Umstände durch einen Geheimdienstmitarbeiter sein. Fraglich ist vor diesem Hintergrund die Einordnung des Beschlusses einer verdeckten Operation.

Vergleichend heranziehen lässt sich insoweit die Frage nach der Behandlung des sog. Scalping. Dabei beschließt ein Marktteilnehmer, etwa ein Analyst, ein bestimmtes Wertpapier zu empfehlen und erwirbt es noch vor der Empfehlung selbst. Sahen insoweit noch das Landgericht Frankfurt a.M.[53] und das Landgericht Stuttgart[54] den Tatbestand des § 14 Abs. 1 Nr. 1 WpHG als erfüllt an, lehnte der BGH dies unter Aufhebung des Urteils des Landgerichts Stuttgart ab.[55] Denn der Begriff der präzisen Information weise im allgemeinen Sprachgebrauch einen Drittbezug auf. Daran fehle es – anders als beim sog. Frontrunning[56] – beim Scalping, da sich der Täter nicht über einen selbst gefassten Gedanken informieren könne.[57] Ob sich an dieser Einordnung etwas durch die *Georgakis*-Entscheidung des EuGH[58] geändert hat, wird unterschiedlich beantwortet.[59] In dem zugrunde liegenden Fall hatten Angehörige der Familie Georgakis beschlossen, die Parnassos-Aktie mittels zwischen ihnen selbst getätigten Geschäften zu stützen, um den Kurs insoweit künstlich zu erhöhen. Der EuGH entschied, dass die Kenntnis vom Vorliegen einer solchen Entscheidung und ihres Inhalts für diejenigen, die an ihr beteiligt waren, eine Insider-Information i. S. von Art. 1 Abs. 1 der Insiderrichtlinie[60] darstellt.[61] Diejenigen, die darin einen Widerspruch zu den von dem BGH aufgestellten Grundsätzen betreffend das Scalping nicht zu erkennen vermögen, führen an, dass in dem der *Georgakis*-Entscheidung zugrunde liegenden Fall ein Drittbezug bestehe. Denn insoweit handelten mehrere Personen gemeinschaftlich.

Wie beim Scalping steht auch bei einer verdeckten Operation zu Beginn ein Beschluss als subjektives Element. Überträgt man die dazu diskutierten Grundsätze, so besteht ein Drittbezug zwar nicht für den einzelnen Mitarbeiter, der die Operation beschließt. Eine Information liegt aber dann vor, wenn der Beschluss in der Hand mehrerer Mitarbeiter

52 Assmann, in: Assmann/U.H. Schneider, WpHG, 5. Aufl., 2009, § 13 Rn. 13; Schwark/Kruse (Fn. 48), § 13 WpHG Rn. 15 m.w.N.; Bürgers, BKR 2004, 424; a.A. KK-WpHG/Klöhn, 2. Aufl. 2014, § 13 Rn. 71 f.

53 Beschl. v. 9.11.1999 – 5/2 Kls 92 Js 23140.2/98 (P 2/98), NJW 2000, 301, 302 mit Anm. Weber, NJW 2000, 562 ff. = DStR 2000, 393 mit Anm. Hergeth.

54 Urt. v. 30.8.2002 – 6 KLs 150 Js 77452/00, BKR, 167, 169 ff.

55 Urt. v. 6.11.2003 – 1 StR 24/03, BGHSt 48, 373 = NJW 2004, 302.

56 Dabei werden Eigengeschäfte in Kenntnis von bevorstehenden Transaktionen anderer Personen in Insiderpapieren getätigt (s. § 13 Abs. 1 Satz 4 WpHG).

57 Urt. v. 6.11.2003 – 1 StR 24/03, BGHSt 48, 373, 379 = NJW 2004, 302, 303; dem zumindest für das neue Recht folgend Schwark/Kruse (Fn. 48), § 13 WpHG Rn. 16.

58 Urt. v. 10.5.2007 – C-391/04, EuZW 2007, 572.

59 Dafür Assmann (Fn. 52), § 13 Rn. 10; Klöhn, (Fn. 52), § 13 Rn. 16; dagegen Schwark/Kruse (Fn. 48), § 13 WpHG Rn. 16b.

60 Richtlinie 89/592/EWG des Rates vom 13. November 1989 zur Koordinierung der Vorschriften betreffend Insider- Geschäfte, ABl. EG L 334 v. 18.11.1989 S. 30 ff.

61 Urt. v. 10.5.2007 – C-391/04, Rz. 33, EuZW 2007, 572, 573.

liegt oder ein anderer Mitarbeiter, der nicht an der Beschlussfassung beteiligt war, in Kenntnis des Beschlusses handelt.

Akut kann daher auch die Frage nach sog. gestreckten Sachverhalten werden. Denn nach dem *Daimler*-Urteil des EuGH[62] und BGH[63] kann, soweit dabei ein bestimmter Umstand verwirklicht oder ein bestimmtes Ereignis herbeigeführt werden soll, eine präzise Information i. S. der Marktmissbrauchsrichtlinie[64] nicht nur dieser Umstand oder dieses Ereignis sein, sondern auch die mit der Verwirklichung des Umstands oder Ereignisses verknüpften Zwischenschritte dieses Vorgangs,[65] mithin der Beschluss einer verdeckten Operation.

Bloße Gerüchte hingegen sind keine Insiderinformationen.[66] Handelt ein Geheimdienstmitarbeiter daher lediglich aufgrund eines unsicheren „Tipps", so liegt darin kein Verstoß gegen § 14 Abs. 1 Nr. 1 und 2 WpHG.

b) Emittentenbezug

Ein Emittentenbezug wird angenommen, wenn die Information die Vermögens- und Finanzlage, die Ertragslage, den allgemeinen Geschäftsverlauf oder die personelle/organisatorische Struktur des Emittenten betrifft.[67] Dabei kommt es freilich sehr stark auf den Einzelfall an. Der Information können unternehmensinterne oder -externe Sachverhalte zugrunde liegen.

Unternehmensinterna sind etwa Umsatzsteigerungen, wesentliche Vertragsabschlüsse oder Erfindungen und Entdeckungen (z.B. Ölfunde) eines Unternehmens, Produktfehler, Gewinnschätzungen oder bevorstehende Übernahmeangebote. Interne Sachverhalte sind ferner das im Fokus von Geheimdiensten stehende[68] technische Know-how eines Unternehmens, Fertigungstechniken, wirtschaftspolitische Strategien, Unternehmens-, Markt- und Absatzstrategien, Zielrichtungen und Methoden der Forschung, Wettbewerbsstrategien, Preisgestaltung und Konditionen sowie Zusammenschlüsse und Absprachen von Unternehmen. Dabei besteht ein klarer Emittentenbezug. Ob die Informationserlangung durch Gelegenheitsfunde oder mittels gezielter Wirtschaftsspionage erfolgt, kann hierbei dahinstehen.

Als externe Umstände kommen etwa kartellrechtliche Untersagungen, Einleitungen von Ermittlungsverfahren oder Gerichtsentscheidungen, die für das Unternehmen wesentliche Vorgänge betreffen, in Betracht.[69] Auch Marktdaten bzw. Marktinformationen

62 Urt. v. 28.6.2012 – C-19/11 (Markus Geltl/Daimler AG), NJW 2012, 2787 ff.; dazu Möllers/Seidenschwann, NJW 2012, 2762 ff.; Bingel, AG 2012, 685 ff.

63 Beschl. v. 23.4.2013 – II ZB 7/09, AG 2013, 518, 519; dazu Ihrig/Kranz, AG 2013, 515 ff.

64 Richtlinie 2003/6/EG des europäischen Parlaments und des Rates vom 28. Januar 2003 über Insider-Geschäfte und Marktmanipulation (Marktmissbrauch), ABl. EU L 96 v. 12. 4. 2003, S. 16 ff.

65 EuGH, Urt. v. 28.6.2012 – C-19/11, Rz 40 (Markus Geltl/Daimler AG), NJW 2012, 2787, 2788.

66 Begr. RegE AnSVG, BT-Drucks. 15/3174, S. 34; CESR, Advice on Level 2 Implementing Measures for the proposed Market Abuse Directive, S. 9, Tz. 20; näher Fleischer/Schmolke, AG 2007, 841 ff.

67 Caspari, ZGR 1994, 530, 539; Schwark/Kruse (Fn. 48), § 13 WpHG Rn. 38; offen Klöhn (Fn. 52), § 13 Rn. 124.

68 Siehe Bundesamt für Verfassungsschutz (Fn. 7), S. 7.

69 Vgl. BaFin, Emittentenleitfaden 2009, Ziff. IV.2.2.12, S. 62; Schwark/Kruse (Fn. 48), § 13 WpHG Rn. 38.

werden heute überwiegend als Insiderinformation angesehen,[70] jedenfalls dann, wenn sie sich nur branchenspezifisch, d.h. auf eine bestimmte Reihe von Emittenten, auswirken. Bei Marktdaten handelt es sich um Informationen über die Rahmenbedingungen von Märkten oder über die Märkte selbst, die auch die Verhältnisse von Emittenten und Insiderpapieren – mittelbar – berühren können. Branchenspezifisch sind davon insbesondere Rohstoffpreise. Unterschiedlich wird indes beantwortet, wie Informationen behandelt werden, die sich auch auf Emittenten darüber hinaus auswirken und damit nicht nur auf einige Emittenten begrenzt sind. Dies sind etwa gesamtwirtschaftliche statistische Daten wie Arbeitslosenzahlen, Inflationsraten, Gesetzesvorhaben oder das Rating eines Landes. Aber auch gänzlich marktferne Ereignisse wie Naturkatastrophen, Kriege, Regierungsumbildungen und andere politische Geschehnisse[71] fallen in diese Kategorie.

Soweit deren Kenntnis notwendig ist, um die Gefahr eines bewaffneten Angriffs auf die BRD, USA bzw. das Vereinigte Königreich oder der Begehung internationaler terroristischer Anschläge mit unmittelbarem Bezug zur BRD, der USA bzw. zum Vereinigten Königreich zu erkennen und abzuwenden, unterfallen sie den Sammlungsaufträgen des BND nach § 5 Abs. 1 Satz 3 G 10,[72] der NSA nach FISA[73] bzw. dem MI6 oder dem GCHQ nach RIPA.[74] Der Übergang zu branchenspezifischen Informationen ist allerdings fließend. Nur wenn man dem Tatbestandsmerkmal „Emittentenbezug" keine eigenständige Bedeutung zumisst, lassen sich solche nicht branchenbezogenen Informationen als Insiderinformationen einordnen. Die besseren Gründe sprechen dafür.[75] Geheim(haltungsbedürftig)e Informationen können daher auch unternehmensexterne Sachverhalte darstellen. Bei einer beschlossenen Operation als externem Umstand kommt es insoweit auf den Einzelfall an. Gegeben ist dieser sicherlich dann, wenn eine Regierung geputscht werden soll, die zuvor Vermögenswerte des entsprechenden Unternehmens verstaatlicht oder in anderer Weise auf dessen Geschäft eingewirkt hatte. In anderen Fällen bedarf es noch mehr einer gewissen Intensität der Operation. Als marktferne Ereignisse kommen dann entsprechend dem Sammlungs- und Auswertungsauftrag der deutschen Geheimdienste vor allem die – soweit nicht bereits einen unternehmensinternen Sachverhalt betreffend – übrigen Informationen von außen- und sicherheitspolitischer Bedeutung für die BRD[76] in Betracht. In diesem Rahmen kann daher ein Emittentenbezug auch bei Informationen betreffend Putschversuche[77] oder sozialökonomische und politische Trends[78] bestehen.

70 BaFin, Emittentenleitfaden 2009, Ziff. III.2.1.3, S. 32 f.; Schwark/Kruse (Fn. 48), § 13 WpHG Rn. 40 m.w.N.
71 Schwark/Kruse (Fn. 48), § 13 WpHG Rn. 41.
72 Siehe bereits oben II.1.
73 Siehe 50 U.S.C. § 1801(e); dazu auch oben II.2.
74 Section 5(3) RIPA: "a warrant is necessary (a) in the interests of national security; (b) for the purpose of preventing or detecting serious crime; (c) for the purpose of safeguarding the economic well-being of the United Kingdom" oder bei einem vergleichbaren Sachverhalt aus Gründen internationaler Zusammenarbeit; noch weitergehend section 22(2) RIPA; dazu oben II.3.
75 Näher Schwark/Kruse (Fn. 48), § 13 WpHG Rn. 41 und Klöhn (Fn. 52), § 13 Rn. 121 ff.
76 Siehe etwa § 1 Abs. 2 BNDG und oben II.1.
77 Siehe dazu Dube/Kaplan/Naidu (Fn. 6).
78 Siehe Bundesamt für Verfassungsschutz (Fn. 7), S. 7.

c) Eignung zur erheblichen Beeinflussung des Börsen- oder Marktpreises

Die Eignung der Umstände zur erheblichen Beeinflussung des Börsen- oder Marktpreises ist durch eine Ex-ante-Prognose anhand objektiver Kriterien zu bestimmen.[79] Eine solche Eignung ist gegeben, wenn ein verständiger Anleger die Information bei seiner Anlageentscheidung berücksichtigen würde (§ 13 Abs. 1 Satz 2 WpHG). Dies kann jedenfalls dann angenommen werden, wenn ein nicht nur unerheblicher Gewinn mit überwiegender Wahrscheinlichkeit erwartet werden kann.[80] So etwa bei wichtigen Vertragsabschlüssen, Erfindungen und Entdeckungen (z.B. Ölfunde). Auch Informationen betreffend technisches Know-how der Gesellschaft bedürfen eines bestimmten Gewichts. Ebendies gilt auch für Fertigungstechniken, Unternehmens-, Markt- und Absatzstrategien, Zielrichtungen und Methoden der Forschung, Wettbewerbsstrategien, Preisgestaltung und Konditionen sowie Zusammenschlüsse und Absprachen von Unternehmen einschließlich bevorstehender Übernahmeangebote.

Auch Marktdaten können den Börsen- oder Marktpreis erheblich beeinflussen.[81] Dabei ist aber danach zu differenzieren, wie marktnah oder marktfern ein Ereignis ist. Mit zunehmender Marktferne bedarf es mehr an Sorgfalt zu prüfen, ob die Information geeignet ist, den Preis eines Insiderpapiers zu beeinflussen. So bedarf es dafür etwa regelmäßig wenig Begründungsaufwand für eine Leitzinsentscheidung der EZB. Marktferne Ereignisse hingegen sollten von solcher Tragweite sein, dass sie die wirtschaftliche Situation eines Landes nachhaltig zu beeinflussen vermögen – wie etwa bei den Terroranschlägen vom 11. September 2001[82] oder einem Putschversuch.[83] Nichts anderes gilt für wirtschaftspolitische Strategien sowie sozialökonomische und politische Trends von einer gewissen Erheblichkeit.

2. Unbefugte Weitergabe

Entscheidend im Rahmen des § 14 Abs. 1 Nr. 2 WpHG ist die „Unbefugtheit" der Weitergabe. Wann dies der Fall ist, wird in der Literatur kontrovers diskutiert. Häufig wird dafür dahingehend unterschieden, ob eine Weitergabe an betriebsexterne Personen oder rein innerbetrieblich erfolgt.[84] Unbefugtheit wird aber jedenfalls dann angenommen, wenn die Weitergabe erforderlich ist,[85] wobei es bei der Weitergabe an Betriebsexterne auch noch auf andere Umstände ankommen kann, wie etwa die Sensibilität der entsprechenden Information.[86] Dabei bezieht sich die Erforderlichkeit der Weitergabe an Betriebsinterne darauf, dass es ihnen möglich sein muss, ihren Beruf ordnungsgemäß auszuüben und die Interessen ihres Unternehmens wahrzunehmen. Art. 3 lit. a) Marktmissbrauchsrichtlinie schreibt insoweit vor, dass es den Verbotsadressaten zu untersagen ist,

79 Assmann (Fn. 52), § 13 Rn. 58 ff.; Schwark/Kruse (Fn. 48), § 13 WpHG Rn. 44; Klöhn (Fn. 52), § 13 Rn. 165.
80 Assmann (Fn. 52), § 13 Rn. 60; Schwark/Kruse (Fn. 48), § 13 WpHG Rn. 50 m.w.N.
81 Schwark/Kruse (Fn. 48), § 13 WpHG Rn. 57.
82 Schwark/Kruse (Fn. 48), a.a.O.
83 Siehe dazu Dube/Kaplan/Naidu (Fn. 6).
84 Schwark/Kruse (Fn. 48), § 14 WpHG Rn. 47 m.w.N.
85 Assmann (Fn. 52), § 14 Rn. 74; Schwark/Kruse (Fn. 48): „aus betrieblichen Gründen erforderlich".
86 Siehe EuGH, Urt. v. 22.11.2005 – C-384/02, Rz. 38, Slg. 2005, I-9939; dabei ging es um die Information über eine Fusion zwischen zwei börsennotierten Gesellschaften.

Insider-Informationen an Dritte weiterzugeben, soweit dies nicht im normalen Rahmen der Ausübung ihrer Arbeit oder ihres Berufes oder der Erfüllung ihrer Aufgaben geschieht. Mit Blick auf den entsprechenden Art. 3 lit. a) der Insiderrichtlinie urteilte der EuGH, dass eine Weitergabe einer Insiderinformation nur dann gerechtfertigt sei, wenn sie für die Ausübung einer Arbeit oder eines Berufes oder für die Erfüllung einer Aufgabe unerlässlich ist und den Grundsatz der Verhältnismäßigkeit beachtet.[87] Ob damit § 14 Abs. 1 Nr. 2 WpHG restriktiver zu handhaben ist, kann vorliegend dahinstehen.

Die „Unbefugheit" der Weitergabe von geheim(haltungsbedürftig)en Informationen ergibt sich insoweit bereits aus den nachrichtendienstlichen Bestimmungen, die konkretisierend herangezogen werden können. Danach darf ein Nachrichtendienst Informationen einschließlich personenbezogener Daten an öffentliche Stellen übermitteln, wenn dies zur Erfüllung seiner Aufgaben oder aus Sicherheitsgründen erforderlich ist (vgl. § 9 Abs. 1 BNDG, § 19 Abs. 3 BVerfSchG). Die Parallelen zu dem oben dargestellten Verständnis von „unbefugt" drängen sich auf. Nichts anderes besagt die sog. *need-to-know*-Regel. Danach werden an eine Person nur die Informationen weitergegeben, die von ihr auch wirklich nur für ihre Arbeit benötigt werden. Näheres bestimmt auch die Anlage 6 zur VSA. Danach sind etwa innerhalb eines Hauses „VS-VERTRAULICH" oder höher eingestufte VS von Hand zu Hand weiterzugeben oder durch Boten zu befördern (Nr. 1.1 Anlage 6 VSA). Für die Weitergabe an Privatpersonen wird insoweit nach Nr. 4.5 Anlage 6 VSA bestimmt, dass sie nur dann Kenntnis von VS erhalten dürfen, wenn dies im staatlichen Interesse (z.B. zur Durchführung eines staatlichen Auftrags) erforderlich ist. Sie sind, wenn es sich um VS-VERTRAULICH oder höher eingestufte VS handelt, zuvor zu überprüfen.

IV. Verbot der Marktmanipulation

Es ist verboten, unrichtige oder irreführende Angaben über Umstände zu machen, die für die Bewertung eines Finanzinstruments erheblich sind, oder solche Umstände entgegen bestehenden Rechtsvorschriften zu verschweigen, wenn die Angaben oder das Verschweigen geeignet sind, auf den inländischen Börsen- oder Marktpreis eines Finanzinstruments oder auf den Preis eines Finanzinstruments an einem organisierten Markt in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum einzuwirken (§ 20a Abs. 1 Satz 1 Nr. 1 WpHG).

§ 20a Abs. 1 Satz 1 Nr. 1 Alt. 1 WpHG käme etwa dann in Betracht, wenn ein Mitarbeiter eines Geheimdienstes behauptet, Kenntnis von einem wichtigen Vertragsabschluss, einer wichtigen Erfindung oder Entdeckung (z.B. Ölfunde) erlangt zu haben oder eine geheime Operation (etwa ein Putschversuch) sei beschlossen worden, dies aber nicht der Wahrheit entspricht, oder entsprechende Angaben nur unvollständig gemacht werden. Dies können im Einzelfall durchaus auch bewertungserhebliche Umstände sein. Wird dafür teilweise in Anlehnung an das US-amerikanische Börsenrecht darauf abgestellt, ob die betreffende Information Einfluss auf die Investitionsentscheidung eines verständigen

87 EuGH, Urt. v. 22.11.2005 – C-384/02, Rz. 34, Slg. 2005, I-9939.

Anlegers mit durchschnittlicher Marktkenntnis nehmen wird,[88] weisen andere insoweit auf das Erfordernis eines Sachverständigengutachtens hin.[89] Eine Konkretisierung erfolgt jedenfalls durch § 2 Abs. 2 bis 4 MaKonV. Danach sind regelmäßig nach § 15 Abs. 1 Satz 1 veröffentlichungspflichtige Insiderinformationen (sog. Ad-hoc-Publizität) auch bewertungserheblich (§ 2 Abs. 2 MaKonV). Da dies nur Informationen sind, die den Emittenten unmittelbar betreffen, sind allgemeine Marktdaten im Rahmen des § 20a WpHG nicht erheblich, es sei denn, sie wirken sich in spezifischer Weise auf den Kurs des Emittenten aus.[90] Bei Bewertungserheblichkeit kann grundsätzlich auch davon ausgegangen werden, dass die Mitteilung geeignet ist, den Kurs des betreffenden Vermögenswerts zu beeinflussen.[91]

Daher können auch Informationen betreffend technisches Know-how, Fertigungstechniken, wirtschaftspolitische Strategien, sozialökonomische und politische Trends, Unternehmens-, Markt- und Absatzstrategien, Zielrichtungen und Methoden der Forschung, Wettbewerbsstrategien, Preisgestaltung und Konditionen sowie Zusammenschlüsse und Absprachen von Unternehmen[92] (einschließlich bevorstehender Übernahmeangebote) bewertungserhebliche Umstände sein.

§ 20a Abs. 1 Satz 1 Nr. 1 Alt. 2 WpHG kommt demgegenüber bei Mitarbeitern von Geheimdiensten schon deswegen nicht in Betracht, da sie üblicherweise nicht Adressat gesellschafts- und kapitalmarktrechtlicher Publizitätspflichten sind. Vielmehr bedarf es gerade des Verschweigens *aufgrund* bestehender Rechtsvorschriften wie der VSA.

Eher denkbar ist ein Verstoß gegen § 20a Abs. 1 Satz 1 Nr. 2 WpHG. Danach ist es verboten, Geschäfte vorzunehmen oder Kauf- oder Verkaufsaufträge zu erteilen, die geeignet sind, falsche oder irreführende Signale für das Angebot, die Nachfrage oder den Börsen- oder Marktpreis von Finanzinstrumenten zu geben oder ein künstliches Preisniveau herbeizuführen. Ein Ausschluss wegen zulässiger Marktpraxis nach Abs. 2 erscheint dabei schwer vorstellbar.

§ 20a Abs. 1 Satz 1 Nr. 3 WpHG verbietet es, sonstige Täuschungshandlungen vorzunehmen, die geeignet sind, auf den inländischen Börsen- oder Marktpreis eines Finanzinstruments oder auf den Preis eines Finanzinstruments an einem organisierten Markt in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum einzuwirken. Darunter wird etwa das bereits angesprochene sog. Scalping gefasst (vgl. auch § 4 Abs. 3 Nr. 2 MaKonV).[93] Entsprechend kann sich auch die eine geheime Operation beschließende Person marktmanipulativ verhalten.

88 Schwark (Fn. 48), § 20a WpHG Rn. 19; s. auch Vogel, in: Assmann/U.H. Schneider, WpHG, 5. Aufl., 2009, § 20a Rn. 76; a.A. Sorgenfrei, wistra 2002, 321, 324 ff.; Altenhain, BB 2002, 1874, 1878; kritisch auch Weber, NZG 2004, 23, 27 f.

89 Vogel (Fn. 88), § 20a Rn. 76.

90 Schwark (Fn. 48), § 20a WpHG Rn. 20.

91 Altenhain, BB 2002, 1874, 1877; Schwark (Fn. 48), § 20a WpHG Rn. 27.

92 Siehe Bundesamt für Verfassungsschutz (Fn. 7), S. 7.

93 BGH, Urt. v. 6.11.2003 – 1 StR 24/03, BGHSt 48, 373; Schwark/Kruse (Fn. 48), § 13 WpHG Rn. 16b.

V. Zusammenfassung und Schluss

Über eine Strafbarkeit wegen der Verletzung des persönlichen Lebens- und Geheimbereichs (§§ 201 ff. StGB), insbesondere der Verwertung fremder Geheimnisse (§ 204 StGB), hinaus, kommt für Mitarbeiter von Geheimdiensten auch ein Verstoß gegen das Verbot von Insidergeschäften (§ 14 Abs. 1 WpHG) und das Verbot der Marktmanipulation (§ 20a Abs. 1 WpHG) in Betracht. Dabei stellen Insiderinformationen über beschlossene Putschversuche freilich (nur) die Spitze des Eisbergs dar. Wichtige Vertragsabschlüsse, Erfindungen und Entdeckungen (z.B. Ölfunde) sind mit entsprechender Begründung ebenfalls als Insiderinformationen zu behandeln wie Informationen betreffend technischen Know-hows, Fertigungstechniken, wirtschaftspolitische Strategien, sozialökonomische und politische Trends, Unternehmens-, Markt- und Absatzstrategien, Zielrichtungen und Methoden der Forschung, Wettbewerbsstrategien, Preisgestaltung und Konditionen sowie Zusammenschlüsse und Absprachen von Unternehmen.[94]

Handelt der Mitarbeiter vorsätzlich oder leichtfertig, kann er sich über § 38 Abs. 1 WpHG strafbar machen. Im Fall des § 14 Abs. 1 Nr. 2 WpHG bedarf es dafür der Einordnung des Mitarbeiters als Primärinsider i. S. des § 38 Abs. 1 Nr. 2 WpHG.[95] In Betracht kommt insoweit dessen berufliche Stellung (§ 38 Abs. 1 Nr. 2 lit. c WpHG). Ein vorsätzliches Handeln wird mit Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe bedroht, ein leichtfertiges Handeln im Fall des § 14 Abs. 1 Nr. 1 WpHG mit Freiheitsstrafe bis zu einem Jahr oder Geldstrafe. Daneben kommt ein Berufsverbot (§ 70 StGB)[96] und die Pflicht zur Herausgabe des durch das Insidergeschäft erzielten Gewinns (§ 73 StGB)[97] in Betracht. Bei einem Verstoß gegen § 20a Abs. 1 WpHG gilt: Handelt der Mitarbeiter vorsätzlich, kann er sich über §§ 38 Abs. 2, 39 Abs. 1 Nr. 1 oder 2 oder Abs. 2 Nr. 11 WpHG strafbar machen.[98] Ein vorsätzliches Handeln wird mit Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe bedroht.

Dabei ist freilich zu beachten, dass regelmäßig große Schwierigkeiten bestehen werden, entsprechende Handlungen nachzuweisen. Die Dunkelziffer könnte deswegen hoch sein. Ein Whistleblowing ist, wie die Veröffentlichungen im Fall *Snowden* zeigen, aber stets denkbar.

94 Siehe Bundesamt für Verfassungsschutz (Fn. 7), S. 7.

95 Anderenfalls handelt der Mitarbeiter jedenfalls ordnungswidrig (§ 39 Abs. 2 Nr. 3 WpHG). Dann beträgt die angedrohte Geldbuße bis zu 200 000 Euro (§ 39 Abs. 4 WpHG).

96 Siehe bereits Assmann (Fn. 52), § 14 Rn. 199; Schwark/Kruse (Fn. 48), § 14 WpHG Rn. 98.

97 BGH, Beschl. v. 27.1.2010 – 5 StR 224/09, NJW 2010, 882.

98 Dann handelt der Mitarbeiter auch ordnungswidrig. Bei leichtfertigem Handeln kann auch der Ordnungswidrigkeitentatbestand des § 39 Abs. 2 Nr. 11 WpHG erfüllt sein. Die angedrohte Geldbuße beträgt bis zu 1 Mio. Euro (§ 39 Abs. 4 WpHG).