

Cyberspionage – Sicherheit vs. Datenschutz und Freiheit

von Stefanie Lürer

Seminar „Digitale Überwachung und Cyberspionage: Deutsch-Französische Perspektive“ in Paris, 22.–23. September 2016

Cyberspionage beschäftigt seit den Snowden-Enthüllungen und dem Skandal um Angela Merkels Überwachung durch den US-Geheimdienst die Öffentlichkeit. Die Schweizer Bevölkerung hat sich gleichwohl mit dem Referendum vom 25. September 2016 für eine Ausweitung der Befugnisse ihres Geheimdienstes bei der Überwachung von Telefonaten und digitaler Kommunikation ausgesprochen.¹ Ihr ist also an einer Ausweitung der Spionagetätigkeit, am Kampf um den Informationsvorsprung gelegen.

Definiert wird Spionage als „Tätigkeit für einen Auftraggeber oder Interessenten [...] zur Auskundschaftung militärischer, politischer oder wirtschaftlicher Geheimnisse“.² Die Tagung „Cyberspionage“ trifft den Nerv einer Zeit, in der wir dank moderner Technik jederzeit blitzschnell eine Fülle von Daten miteinander austauschen können. Diesen Informationsflüssen steht das Streben gegenüber, Gefahren und Bedrohungen durch kriminelle Vereinigungen und Terrorismus abzuwehren. Die Frage lautet daher: Wie sind die Rechte auf Datenschutz, Privatsphäre, Vergessen im Netz und freie Meinungsäußerung mit dem Streben nach einem Informationsvorsprung zur Sicherheitsgewährleistung in Einklang zu bringen? Die Lösung erfordert auf staatlicher wie auf internationaler Ebene regulatorische und institutionelle Maßnahmen.

Zu Beginn der Tagung wurde der Stummfilm *Spione* (1928) von Fritz Lang gezeigt, in dem sich die Geheimagenten bereits moderner Telekommunikationsmethoden bedienen. Mit Blick auf die historische Fortentwicklung im Spionagefilmgenre erläuterte BASTIAN GASCHO (Berlin) anschließend die Thematik der Spionage aus filmwissenschaftlicher Sicht.

Gascho legte den Schwerpunkt auf das *storytelling*, dem er eine Art Propagandafunktion zuordnet, da es die Grenzen von Gut und Böse definiere, die im Kontext des Ausspähens immer verschwommen seien. Immaterielle Vorgänge wie

z.B. eine Täuschung durch Doppelspione, zwischenmenschliches Vertrauen und Misstrauen, Geheimnisse und Verrat sowie der Akt der Informationsbeschaffung stehen im Zentrum des Spionagefilmgenres und verlangen eine bildliche Darstellung. Um den Spionageakt zu verdeutlichen, erläuterte Gascho, werden technische Mittel herangezogen, die im Film sichtbar sein müssen, obwohl derartige Abläufe in der realen Welt aber unbemerkt geschehen. Die Welt werde aber trotz der offensichtlichen Darstellung immer im Geheimen gerettet. Entsprechend stelle sich die Frage, was vom Film auf die Wirklichkeit übertragen werden könne.

Nach dieser bildlichen Einführung ins Thema diene der zweite Tag der politikwissenschaftlichen und rechtswissenschaftlichen Betrachtung von Cyberspionage. Am Vormittag befasste sich das erste Panel mit der Regulierung von Geheimdienstaktivitäten. CHRISTIAN DJEFFAL (Berlin) präsentierte die juristische Sicht auf IT-Sicherheit durch Regulierung. Mithilfe von Jeremy Benthams Metapher des Panoptikums machte er eine Besonderheit der Cyberüberwachung deutlich: Technisch ist eine ständige Überwachung möglich, eine ganzheitliche Auswertung der gesammelten Daten findet aber nicht statt. Das bedeutet, der Einzelne weiß um eine mögliche Überwachung, er weiß aber nicht, ob und wann genau sie stattfindet. Um Rechtssicherheit zu gewährleisten, so die Forderung von Juristen an den Gesetzgeber, sei nicht nur auf die Überwacher, sondern auch auf die Überwachten der Blick zu richten. Ebenfalls im Zentrum seiner Untersuchung steht das „Privacy-Paradox“. Diesem zufolge werden selbst technisch leicht umzusetzende Sicherheitsmaßnahmen, z.B. am Smartphone, nicht angewendet, obwohl der Schutz der Privatsphäre einen hohen Stellenwert genießt. Zu klären sei also, wie durch verschiedene Methoden der Regulierung zum einen die Überwachten besser geschützt werden können und zum anderen eine Verpflichtung zum Selbstschutz geschaffen werden kann. Damit verbundene Fragen lauten: Welche Methode ist heranzuziehen, welche Menschenrechte sind zu berücksichtigen, wem kann Vertrauen geschenkt werden und wie ist mit der Ungewissheit, ob und wann Überwachung stattfindet, umzugehen?

Welche Regulierungsansätze in der am 21. Oktober 2016 inzwischen beschlossenen Reform des BND-Gesetzes³ verfolgt werden, analysierte aus politikwissenschaftlicher Perspektive THORSTEN WETZLING (Berlin). Bemerkenswert sei, dass dem Großteil der BND-Arbeit, die aus digitaler Informationssammlung im Ausland besteht, eine gesetzliche Grundlage bislang fehle. Zudem finde eine gerichtliche Überprüfung der Maßnahmen faktisch nicht statt. Als Grund und Anlass zur Kritik nennt er in gleichem Maße die rechtsstaatlich bedenkliche Geheimhaltung der Eingriffshandlungen und die Nichtunterrichtung der Betroffenen. Auch die parlamentarische Überwachung der Geheimdienste durch fünf verschiedene Überwachungskomitees sei befremdlich. Eine Befragung der Entscheidungsträger dieser Komitees habe ergeben, dass diese keine spezielle Aus- und Fortbildung zum Grundrechtsschutz erhalten und sehr wenig Zeit zur Entscheidungsfindung haben. Das belege, dass Gesetze nur wirksam sein könnten, wenn der institutionelle Rahmen stimme. Die Geheimdienstüberwachung durch die

Regierung führte zurück zum Aspekt des Vertrauens: Ist unsere Regierung in der Lage, individuelle Daten durch geheime Reporte zu schützen? Eine Reform der bestehenden gesetzlichen Basis sei zwingend notwendig, um den BND rechtsstaatlich einzubetten. Die Erfolgsaussichten seien aber fraglich, da die vorliegende Reform ein sehr komplexes Gesetz geschaffen habe. Dessen Schutzniveau hänge beispielsweise von der Nationalität des Überwachten ab, und es sehe keine Begrenzung der erhebungsfähigen Datenmenge vor.

In der folgenden angeregten Diskussion kam das Plenum auf die Themen Eigenverantwortung beim Datenschutz, private Überwachungstechnik und das Niveau der Sicherheit zurück, die gesetzlich geschützt werden müsse. Zudem ging es um die unterschiedliche Behandlung aufgrund der Staatsangehörigkeit. Auch wurde diskutiert, ob die IP-Adresse aufgrund ihres nicht unbedingt einer Nation zuzuordnenden, serverbezogenen Charakters als Unterscheidungskriterium für den territorialen Anknüpfungspunkt von Gesetzen taugt.

Das zweite Panel widmete sich der institutionellen Struktur und Überwachung der Geheimdienste in Deutschland und in Frankreich. FRANZISKA BANTLIN (Freiburg) erläuterte sehr ausführlich, in welche Überwachungsstruktur der deutsche Geheimdienst eingebettet ist. Darin fungiert die Regierung als Intermediär, da sie die gewonnenen Informationen verwaltet. Bantlin kritisierte, dass die Kontrolle durch das Parlamentarische Kontrollkomitee und die G10-Kommission⁴ aufgrund der institutionellen Struktur keiner unabhängigen und neutralen gerichtlichen Prüfung gleichkomme. Den Grund dafür sieht Bantlin in der Geheimhaltung der Maßnahmen wie auch in der fehlenden Kenntnis der Überwachten, die das Anrufen eines Gerichts faktisch vereitle. Aber auch der Umstand, dass die Regierung die Informationen, die überprüft werden dürfen, auswähle und somit eine asymmetrische Informationslage bestehe, erschwere eine rechtliche Überprüfung.

Den institutionellen und technischen Rahmen der französischen geheimdienstlichen Überwachung sowie deren Kontrolle stellt FÉLIX TRÉGUER (Paris) anhand eines historischen Überblicks vor. Er befand, dass die gesetzliche Grundlage zur Informationserhebung im Verhältnis zu den technischen Möglichkeiten zu lückenhaft sei. Konkret bezeichnete er sie als „alegal“, womit gemeint ist, dass die Praxis der Informationssammlung zwischen Legalität und Illegalität steht. Er zeigte außerdem viele Widersprüche zwischen Spionage und ihrer Überwachung auf und verwies im Kontext der Snowden-Enthüllungen auf den Journalismus als überwachte Überwachungsinstanz. Durch die Überwachung der Journalisten werde das Recht auf Pressefreiheit verletzt und auch deren Tauglichkeit als unabhängige Wächter in Frage gestellt. Bei der Informationserlangung seien Journalisten außerdem mit den Problemen konfrontiert, dass Hacking – wie im Fall Snowden – als Straftat gelten könne und damit auch wieder die Pressefreiheit durch die Strafandrohung beeinträchtigt werden könne, womit ihre Überwachungsfunktion auf dem Spiel stehe. Tréguer äußerte Kritik am Gesetzgebungsverfahren, das weitestgehend unbeachtet geblieben sei, obwohl es ein weites Feld für staatliche

Eingriffe eröffne.

Es folgte eine animierte Diskussion zur Frage, ob Geheimdienstüberwachung überhaupt legal zu verwirklichen sei, mit dem Ergebnis, eine Anpassung der Regulierung sei nur begrenzt möglich. Schließlich könnten Schutzmechanismen, die durch NGOs, Parlamente und Gerichte gewährleistet werden, mit Verweis auf die Sicherheit (Stichwort Terrorismusbekämpfung) umgangen werden.

Im dritten Panel, das sich dem europäischen und internationalen Menschenrechtsschutz widmete, plädierte LAYLA KRISTINA JABER (Heidelberg) dafür, die Rechte auf internationaler Ebene, die sich aus dem Völkergewohnheitsrecht und verschiedenen internationalen und regionalen Abkommen ableiten, auch auf die Rechte im Netz zu übertragen. Es handelt sich insbesondere um Rechte, die das Individuum vor staatlicher Überwachung im Netz schützen, wie das Recht auf Privatsphäre, auf Datenschutz und auf Vergessen im Netz. Allgemeine Menschenrechte, die auch im Netz gelten, seien ebenfalls zu schützen, etwa die Meinungs- und Pressefreiheit sowie die freie Religionsausübung. Die Grenze für staatliche Eingriffshandlungen sei stets die Rechtsstaatlichkeit – problematisch findet Jaber daher, dass der Datenaustausch zwischen den nationalen Geheimdiensten durch verwaltungsinterne Vorschriften geregelt wird. Anhand zahlreicher Beispiele erklärte sie schließlich die externen Überwachungsfunktionen der Presse (*watchdog*) und die Sekundäreffekte der Sicherheitspolitik (*chilling effect*), die sich in der Selbstzensur aus Angst vor staatlichen Repressionen äußern könnten.

Im zweiten Vortrag diskutierte SAHRA GOLGHALYANI (Göttingen) die Ebene des internationalen Menschenrechtsschutzes, den der International Covenant on Civil and Political Rights (ICCPR) verspricht. Als historisch bemerkenswert hob sie hervor, dass bereits seit 1968 die Frage gestellt werde, wie sich der technische Fortschritt auf den Menschenrechtsschutz auswirke. Konkret beleuchtete sie die internationale Regelung in Artikel 17 des ICCP und analysierte die Grenzen ihrer Anwendbarkeit und ihre Auslegung. Im Fokus standen auch für sie die gesetzliche Ermächtigungsgrundlage, die Überwachung durch unabhängige Kontrollorgane und die Unterbindung von Massenspionage bei gleichzeitiger Förderung der nationalen Sicherheit. Frau Golghalyani vertrat die Auffassung, dass der von Art. 17 ICCP vorgesehene multinationale völkerrechtliche Schutz binationalen Datenschutzabkommen vorzuziehen sei, da er einen umfassenden Menschenrechtsschutz ermögliche. Letzterer müsse aufgrund der Globalisierung grundsätzlich auf internationaler Ebene erfolgen.

Das letzte Panel der Tagung widmete sich dem territorialen Anknüpfungspunkt des Schutzes der digitalen Menschenrechte und deren institutioneller Umsetzung. MILAN TAHRAOUI (Paris / Berlin) ergründete den extraterritorialen Menschenrechtsschutz, also die Kompetenz eines Staates, außerhalb seines Gebiets entsprechende Maßnahmen zu ergreifen. Er soll der Gewährleistung eines hohen

Schutzniveaus unter gleichzeitiger Beachtung des staatlichen Sicherheitsauftrages im Kampf gegen Terrorismus und Kriminalität dienen. Im Hinblick auf das Internet werfe das Probleme auf, da die Digitalisierung global erfolge und somit Regulierung und gerichtliche Überprüfung auf drei Ebenen (national, europäisch, international) einschlägig sein könne. Auch die Koexistenz unterschiedlicher Schutzniveaus sei möglich. Ein Regulierungsproblem stelle zudem die Vielfalt privater Akteure, etwa der Telekommunikationsanbieter, dar. Die Zuständigkeit für solche Sachverhalte könne dann beim internationalen Wirtschafts- oder Bankenrecht liegen. Fest steht für Tahraoui, dass sich der Gebietsbegriff im digitalen Bereich von dem des Staatsgebiets unterscheiden muss, da es sich beim Datenverkehr in der Regel um multinationale Kooperationen handelt.

CLÉMENT PERARNAUD (Paris) forscht zur Lobbyarbeit und ihrem Einfluss auf die Gesetzgebung für die *General-data-protection-Reform*⁵ auf europäischer Ebene. Er nutzt dazu verschiedene Analyseplattformen, die den Lobbyeinfluss im Rahmen des europäischen Konsultationsverfahrens ausgewertet haben. So veranschaulichte er, wie unterschiedlich Gesetzesverhandlungen in Frankreich und Deutschland verlaufen und wie stark der Lobbyeinfluss in der digitalen Welt ausfällt. Es könne unterstellt werden, resümierte Perarnaud, dass derjenige, der die Technik beherrscht, gleichzeitig ihre Regulierung bestimmt.

Viele neue Ideen, aber auch Kritik an der bisherigen regulativen und institutionellen Praxis Frankreichs und Deutschlands sowie auf internationaler Ebene wurden auf dieser pluridisziplinären, multinationalen Tagung im Herzen von Paris entwickelt, die Filmwissenschaften, Politikwissenschaften und Rechtswissenschaften miteinander in den Dialog gebracht hat. Bemerkenswert war, wie die Problembetrachtung und -lösung je nach Fachbereich und nationaler Ausbildung variiert. So legt die Politikwissenschaft ihren Fokus auf die institutionelle und die lebensweltliche Umsetzung von Gesetzen, indem sie sich u.a. auf Interviews und Meinungserhebungen stützt, wohingegen die Rechtswissenschaft als Erkenntnisquelle primär die Gesetzestexte, deren Analyse und gerichtliche Gewährleistung verwendet. Eine Zusammenführung der Erkenntnisquellen hilft beiden Wissenschaften, sich zu verbessern und weiterzuentwickeln. Der multilinguale, interdisziplinäre Austausch regte dazu an, aus gewohnten (Denk)-Strukturen auszubrechen und somit über den eigenen (disziplinären und nationalen) Tellerrand hinauszuschauen.

Konferenzübersicht:

Moderation: Laurence Meyer

Filmvorführung:

Fritz Lang, Spione

Bastian Gascho (Berlin), Kontinuitäten und Bruchlinien in der Filmischen Repräsentation „analoger“ und „digitaler“ Spionage

Moderation: Anne Peters

1. Panel: Regulatorischer Rahmen

Christian Djeffal (Berlin), IT-Security Through Law

Thorsten Wetzling (Berlin), Eine kritische Würdigung der BND-Reform

2. Panel: Überwachung der Gesetzesanwendung

Franziska Bantlin (Freiburg) Parlamentarische und gerichtliche Kontrolle von Geheimdiensten in Deutschland

Félix Tréguer (Paris), Enduring Illegality & the Snowden Paradox - About a Forgotten Provision of the 2015 French Intelligence Act

Moderation: Emanuel Castellarin

3. Panel: Menschenrechtsschutz durch Europäische und internationale Regelungen

Layla Kristina Jaber (Heidelberg), Verpflichtungen der Staaten aus den internationalen Menschenrechten im Cyberspace, insbesondere aus der EMRK

Sahra Golghalyani (Göttingen), Die geheimdienstliche Ausspähung der Daten und Kommunikation von Individuen im Lichte des ICCPR

4. Panel: Territorialer Anknüpfungspunkt des Schutzes und Institutionelle Umsetzung

Milan Tahraoui (Paris / Berlin), La protection extraterritoriale des droits de l'homme face à la surveillance numérique internationale entre feux croisés

Clément Perarnaud (Paris), De l'adoption du "paquet sur la protection des données" aux négociations de l'accord "Privacy Shield": des contradictions franco-allemandes ?

Robin Caballero / Laurence Meyer / Milan Tahraoui, Schlussworte der Organisatoren

Fußnoten

1[□] Daniel Gerny, Das Nachrichtendienstgesetz auf einen Blick, in: Neue Zürcher Zeitung, 8. August 2016.

2[□] Art. Spionage, in: Duden - Deutsches Universalwörterbuch. Das umfassende Bedeutungswörterbuch der deutschen Gegenwartssprache, Berlin 2016.

3[□] Die Bundesregierung, Bundestag beschließt Gesetz. Klare Regeln für Auslandsaufklärung, 21. Oktober 2016.

4[□] „Die G 10-Kommission entscheidet von Amts wegen als unabhängiges und an keine Weisungen gebundenes Organ über die Notwendigkeit und Zulässigkeit sämtlicher durch die Nachrichtendienste des Bundes (Bundesnachrichtendienst, Bundesamt für Verfassungsschutz, Militärischer Abschirmdienst) durchgeführten Beschränkungsmaßnahmen im Bereich des Brief-, Post- und Fernmeldegeheimnisses nach Artikel 10 des Grundgesetzes (GG).“ (Vgl. Die Bundesregierung, G10-Kommission.)

5[□] “Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).” (Vgl. European Commission, Reform of EU data protection rules.)