# Wer überwacht die digitale Überwachung? Die Kontrolle der Geheimdienste als Gradmesser der Demokratie

*Ronja Kniep*

**Summary:** Who guards the guardians? This is an old question that digital societies must face in a particular way. How can democracies control transnationally and commercially connected surveillance by secret intelligence agencies who draw on complex technical algorithms? The project GUARDINT investigates this question and designs an Intelligence Oversight Index (IOI) that will measure and compare democratic intelligence oversight in different countries.

**Kurz gefasst:** Wer überwacht die Überwacher? Diese alte Frage stellt sich in digitalisierten Gesellschaften in besonderer Weise. Denn wie kontrollieren Demokratien digitale Überwachung, die nicht nur geheim, sondern transnational und kommerziell vernetzt stattfindet und sich dabei komplexer Algorithmen bedient? Das Projekt GUARDINT nimmt sich dieser Frage an und entwickelt dafür den Intelligence Oversight Index (IOI), der die demokratische Kontrolle von Geheimdiensten im internationalen Vergleich vermessen wird.

Einer der Pioniere des Datenschutzes in Deutschland, der Jurist und Philosoph Adalbert Podlech, dachte schon mit Beginn der Computerisierung in den 1970ern über das Problem digitaler Überwachung nach. In mürrischem Tonfall, aber pointiert formulierte er 1976: „Eine Datenschutzregelung ist nur so gut, wie sie das Problem der Geheimdienste regelt, und das bedeutet, daß alle derzeitigen Regelungen schlecht sind." Aus dieser Einsicht können wir noch heute viel lernen: Am Problem digitaler Geheimdienstüberwachung misst sich nicht nur die Qualität des Datenschutzes, sondern die einer Demokratie insgesamt. Wie und durch wen staatliche, aber transnational und kommerziell verflochtene Überwachung kontrolliert wird, sagt etwas darüber aus, wie sich Freiheit, Gewaltenteilung, Repräsentation und Partizipation in Demokratien verwirklichen lassen. In unserem Projekt GUARDINT („Oversight and Intelligence Networks: Who Guards the Guardians?") erheben wir die Ausgestaltung der Geheimdienstkontrolle deshalb zum Gradmesser der Qualität von Demokratie. Damit stellen wir uns der weit verbreiteten Haltung entgegen, Geheimdienste und ihre Überwachungspraktiken stillschweigend als Fremdkörper in demokratischen Gesellschaften zu akzeptieren.

Dies eröffnet die Frage, wie Geheimdienstkontrolle selbst vermessen werden kann. Bei GUARDINT entwickeln wir die Methode für einen Intelligence Oversight Index (IOI), der die Ausgestaltung von Geheimdienstkontrolle in Demokratien ländervergleichend erheben soll. Bevor ich näher auf den IOI eingehe, soll das Objekt der Kontrolle vorgestellt werden: die digitale Überwachung. Häufig wird digitale Überwachung quantitativ charakterisiert, also über die Masse der erhobenen Daten. Doch das greift zu kurz. Die heutigen Formen der Überwachungen zeichnen sich durch eine schwer vermeidbare und allgegenwärtige Produktion mitunter intimer Daten in kommerziellen Verwertungszusammenhängen aus, die auf transnational operierende Geheimdienste mit neuartigen Analysefähigkeiten treffen.

Gerade im Bereich massenhafter digitaler Überwachung – Signals Intelligence (SIGINT) im Fachjargon – gibt es eine lange Tradition der transnationalen Zusammenarbeit, die durch bi- und multilaterale Netzwerke institutionalisiert ist. Besonders bekannt ist das Netzwerk der Five Eyes, bestehend aus den Diensten der USA, Großbritanniens, Kanadas, Australiens und Neuseelands. Sie arbeiten besonders eng zusammen, erheben zuweilen Daten in einem Land, speichern sie in einem anderen und werten sie in einem dritten aus.

Aber auch die europäischen Dienste sind Mitglieder multilateraler Kooperationen, etwa im Club der SIGINT Seniors Europe. Der deutsche Bundesnachrichtendienst (BND) kooperiert laut seinem Präsidenten Bruno Kahl „mit 450 Geheimdiensten in 160 Ländern". Datenaustausch unter SIGINT-Diensten ist nicht die Ausnahme, sondern ein fester Bestandteil der alltäglichen Arbeit. Transnational ist digitale Geheimdienstüberwachung sogar in einem doppelten Sinne: durch die Kooperation der Dienste und durch die für das Internet charakteristische Form der Datenübermittlung in Paketen. Zum Beispiel wird eine E-Mail beim Versand zerstückelt und über unvorhersehbare geografische Routen geleitet. Eine Unterscheidung zwischen in- und ausländischer Kommunikation ist nicht mehr eindeutig möglich, anders als bei der Telefonüberwachung anhand der Vorwahl 0049.

**Ronja Kniep** ist wissenschaftliche Mitarbeiterin in der Forschungsgruppe Politik der Digitalisierung am WZB, zudem hat sie die Co-Leitung des DFG/ORA Projekts „Oversight and Intelligence Networks: Who Guards the Guardians“ (GUARDINT) inne.
*(Foto: Stefanie Klement)*

***ronja.kniep@wzb.eu***

Hier kommt das zweite Merkmal ins Spiel, die Algorithmizität. Der BND und andere Geheimdienste entscheiden auf der Grundlage technischer Algorithmen, ob eine Kommunikation deutschen Staatsbürger:innen oder Ausländer:innen zuzuordnen ist. Hinzu kommen algorithmische Analysen großer Datenmengen, um auffällige Verhaltensmuster schneller oder überhaupt für menschliche Analyst:innen erkennbar zu machen. Dabei haben Geheimdienste begonnen, Künstliche Intelligenz (KI), also maschinelles Lernen, in ihre Überwachungspraxis zu integrieren. Um KI sinnvoll einsetzen zu können, muss aber erst einmal eine große Menge Daten zusammengetragen und integriert werden – was wiederum neue Herausforderungen für den Datenschutz entstehen lässt.

Im Bereich KI spielt die Kooperation der Geheimdienste mit der Privatwirtschaft eine herausragende Rolle. Geheimdienste haben zwar schon immer eng mit Technologieunternehmen zusammengearbeitet, waren dabei aber oft technologisch führend. Heute hat sich die Abhängigkeit der Dienste von privaten Unternehmen vergrößert. Das Merkmal der Kommerzialisierung geheimdienstlicher Überwachung umfasst insgesamt drei Entwicklungen: Firmen wie Google und Facebook haben durch kommerzielle Formen der Überwachung Datenmärkte erschaffen, Unternehmen wie Amazon oder Palantir vergrößern Märkte für Überwachungstools und -infrastrukturen und Firmen wie Booz Allen Hamilton (die Edward Snowden zuletzt beschäftigte) bieten privat angestelltes Überwachungspersonal an. Kommerzielle und geheimdienstliche Anreize für Überwachung verstärken sich gegenseitig und vergrößern die Machtpotenziale digitaler Überwachung insgesamt.

Alle drei Merkmale digitaler Überwachung – Transnationalität, Algorithmizität und Kommerzialisierung – machen die Kontrolle geheimer Dienste noch schwerer. Die transnationalen Kooperationen zwischen den Diensten entziehen sich der Kontrolle durch hauptsächlich national ausgerichtete Institutionen. Auch, weil gemeinsame Vorhaben durch Abmachungen besonders geheim gehalten werden. Der Einsatz von KI erschwert die Nachvollziehbarkeit ohnehin komplexer Überwachungstechnik zusätzlich. Und wenn geheime öffentliche Dienste Aufgaben an private Unternehmen delegieren, unterliegen diese noch weniger Kontrolle. Die Konstellationen und Techniken digitaler Überwachung – insbesondere im Bereich SIGINT – erfordern nicht nur entsprechende Kontrollinstitutionen, sondern auch ihre Erforschung. Zu dieser leistet GUARDINT einen Beitrag.

Trotz der Komplexität betonen Regierungen und Geheimdienste immer wieder selbstbewusst, die „weltbeste“ Geheimdienstkontrolle zu haben, und legitimieren so ihre Überwachungspraxis. Zuletzt behauptete dies Theresa May über die britische Geheimdienstreform 2016. Von Großbritannien, Australien über die USA bis Deutschland – wer hat nun recht und in welcher Hinsicht? Mit unserem Intelligence Oversight Index wollen wir zur Grundlagenforschung und zu politischen Debatten über Geheimdienstkontrolle beitragen. Denn gerade im Sicherheitsbereich werden Kontroversen schnell geschlossen und bestimmte Formen der Kontrolle als undenkbar bezeichnet. Eine Stelle außerhalb des BND mit Zugang zu allen internen Datenbanken? Undenkbar! Aber wenn es die Dänen auch können? Solche Vergleiche, die mit dem IOI an Tiefe und Breite gewinnen, haben etwa in den Verhandlungen zum jüngsten Urteil des Bundesverfassungsgerichts über die BND-Auslandsüberwachung bereits eine wichtige Rolle gespielt. Durch Verweise auf Kontrollpraktiken anderer Länder konnten ähnliche Vorstöße nicht als „unerfüllbar“ abgetan werden. Die Konfrontation mit anderen Ländern kann uns also zeigen, dass erweiterte oder neuartige Formen von Kontrolle weder die Geheimdienstwelt noch die Sicherheit der Bevölkerung zum Einstürzen bringen müssen.

Der IOI definiert Geheimdienstkontrolle als ein Ensemble demokratischer Praktiken, die Geheimdienste und ihre Aktivitäten oder die ihrer Kontrolleur:innen überprüfen, evaluieren oder auch anfechten sowie Öffentlichkeit über sie herstellen. Das Ziel von Geheimdienstkontrolle ist, vergangenes Fehlverhalten aufzudecken und zukünftiges Fehlverhalten zu vermeiden. Dabei unterscheiden wir zwischen delegierten Formen der Kontrolle, die durch parlamentarische, juristische und expertenbasierte Gremien durchgeführt wird, und zivilen For-

men der Kontrolle durch Medien, Nichtregierungsorganisationen (NGOs) oder einzelne Bürger:innen. Dieses breite Verständnis von Geheimdienstkontrolle verbindet Elemente verschiedener Vorstellungen von Demokratie, etwa liberaler, republikanischer und partizipativer Verständnisse. Gleichzeitig trägt ein weiter Begriff von Kontrolle ihren Dynamiken in der Praxis Rechnung. Delegierte Formen der Kontrolle wie Untersuchungsausschüsse kommen tatsächlich nur selten ohne mediale Öffentlichkeit zustande. Die durch Edward Snowden angestoßenen Veröffentlichungen und der daraus folgende NSA-Untersuchungsausschuss des Deutschen Bundestags ist ein prominentes Beispiel.

Was Eigenschaften einer demokratischen Geheimdienstkontrolle sind, möchte ich an drei Fragen verdeutlichen, die wir mit dem IOI erheben. Die erste Frage lautet: Werden Kontrollgremien als Third Parties definiert? Die sogenannte „Third Party Rule" ist eine wichtige Regel der transnationalen geheimdienstlichen Zusammenarbeit. Sie besagt, dass Informationen nur unter dem Vorbehalt geteilt werden sollen, dass der Absender darüber bestimmen kann, ob eine Weitergabe an Dritte erlaubt wird. Oft sind es jedoch nicht nur einzelne Informationen, die in der Logik der Third Party Rule zum geteilten Geheimnis unter Diensten werden und sich einer unabhängigen Kontrolle Dritter entziehen, sondern ganze Programme oder Operationen. Weil ein bedeutender Teil der Geheimdienstarbeit transnational vernetzt stattfindet, sorgt die Gepflogenheit der Third Party Rule dafür, dass sich weite Bereiche einer Kontrolle entziehen. Inwiefern Gremien wie die G 10-Kommission, die über Einschränkungen des Fernmeldegeheimnisses befindet, oder das Parlamentarische Kontrollgremium als Dritte definiert werden, ist daher ein wichtiger Indikator für delegierte Formen von Kontrolle.

Eine zweite Frage, die etwas über die Bedingungen für Geheimdienstkontrolle aussagt, lautet: Wie umfassend haben Länder den Schutz von Whistleblower:innen institutionalisiert? Diese Frage betrifft den Bereich delegierter und ziviler Kontrolle. Damit Insider:innen Missstände in ihren Behörden aufdecken können, bedarf es entsprechender Kanäle und Stellen innerhalb der Dienste. Dass dies durchaus funktionieren kann, zeigte erst kürzlich ein Fall aus Dänemark. Weil der dortige Auslandsgeheimdienst unerlaubterweise dänische Bürger:innen überwachte, wandte sich ein:e Mitarbeiter:in an das dänische Kontrollgremium – mit Konsequenzen: Es folgten drei Suspendierungen, auch des Chefs des Dienstes. Jedoch sind interne Kanäle nicht immer ausreichend, um auf Fehlverhalten aufmerksam zu machen. Das zeigen die Fälle von Geheimdienstmitarbeiter:innen, die erfolglos versuchten, sich intern Gehör zu verschaffen, und sich dann an die Presse wandten. Hier kommt die zivile Kontrolle ins Spiel, nämlich über einen funktionierenden Quellenschutz, unter dem Journalist:innen für Whistleblower:innen erreichbar bleiben.

Eine dritte Frage betrifft die Ausgestaltung von Klagerechten im Bereich geheimer Überwachung. Muss etwa eine Klägerin beweisen, dass sie tatsächlich überwacht wurde, also einen Betroffenheitsnachweis mit stichhaltigen Beweisen erbringen, bevor ein Gerichtsverfahren überhaupt zugelassen wird? Um sich gegen geheime Überwachung zu wehren, muss man sie erst beweisen; das klingt absurd, ist aber in einer Reihe von Demokratien so geregelt, auch in Deutschland und den USA. Für einzelne Bürger:innen, aber auch für Klagekollektive – Organisationen, die sich die Verteidigung von Grundrechten zum Ziel gesetzt haben – sind die Regeln des Zugangs zu juristischen Formen der Kontrolle ein wichtiger Indikator dafür, ob digitale Überwachung in einem Land anfechtbar ist.

Hinter diesen Fragen stehen drei von vielen Indikatoren, die wir für die Vermessung demokratischer Geheimdienstkontrolle entwickeln. Im März 2021 startet die erste Phase der Datenerhebung, zunächst in Deutschland, Frankreich und Großbritannien. Die Vermessung der Geheimdienstkontrolle in diesen und hoffentlich weiteren Ländern verspricht eine Bestandsaufnahme der Kontrolle digitaler Überwachung und vermittelt damit auch einen Eindruck über den Zustand von Demokratie in der Digitalisierung. Denn: Die Qualität von Demokratien zeigt sich gerade dort, wo sie besonders fragil sind, und damit im Umgang mit dem Problem digitaler Geheimdienstüberwachung.

*Literatur*

*Kahl, Bruno: „Rahmenbedingungen und Notwendigkeiten internationaler Kooperation von Nachrichtendiensten". In: Jan-Hendrik Dietrich/Klaus Ferdinand Gärditz/Kurt Graulich (Hg.): Geheimdienste in vernetzter Sicherheitsarchitektur. (Beiträge zum Sicherheitsrecht und zur Sicherheitspolitik). Tübingen: Mohr Siebeck 2020, S. 153–162.*

*Kniep, Ronja: Another Layer of Opacity: How Spies Use AI and Why We Should Talk about It. about:intel, 20. Dezember 2019. Online: https://aboutintel.eu/how-spies-use-ai (Stand 16.02.2021).*

*Podlech, Adalbert: „Gesellschaftstheoretische Grundlage des Datenschutzes". In: Rüdiger Dierstein/Herbert Fiedler/Arno Schulz (Hg.): Datenschutz und Datensicherung. Referate der gemeinsamen Fachtagung der Österreichischen Gesellschaft für Informatik (ÖGI) und der Gesellschaft für Informatik (GI). Köln: Bachem 1976, S. 311–326.*

*Wetzling, Thorsten/Vieth, Kilian: Massenüberwachung bändigen. Gute Rechtsnormen und innovative Kontrollpraxis im internationalen Vergleich. 2019. Online: https://www.stiftung-nv.de/de/publikation/massenueberwachung-baendigen-gute-rechtsnormen-und-innovative-kontrollpraxis-im (Stand 16.02.2021).*

*Das internationale Projekt „Oversight and Intelligence Networks: Who Guards the Guardians?" (GUARDINT) wird von der Deutschen Forschungsgemeinschaft (DFG) im Rahmen der Open Research Area (ORA) gefördert. Der Intelligence Oversight Index (IOI) wird in Zusammenarbeit des WZB mit der Stiftung Neue Verantwortung (SNV) entwickelt und ist ein gemeinsames Produkt von Lina Ewert, Prof. Dr. Jeanette Hofmann, Ronja Kniep, Kilian Vieth, Dr. Thorsten Wetzling und Sarah Naima Roller unter Mitarbeit von Felix Richter und Mouna Smaali. Mehr Informationen zu GUARDINT gibt es unter: www.guardint.org.*