

Akzeptanz staatlicher Überwachung privater Telekommunikation in Deutschland: Ein faktorielles Survey-Experiment

Bruno Albert, Joanna Klauser, Andreas Hammer, Christian Lindenmeier, Sabine Pfeiffer, Dirk Heckmann und Felix Freiling

Zusammenfassung

Der Beitrag untersucht die gesellschaftliche Akzeptanz staatlicher Überwachungsmaßnahmen in Abhängigkeit von deren technischer und rechtlicher Ausgestaltung sowie dem Kontext ihrer Umsetzung. Zu diesem Zweck wurde ein faktorielles Survey-Experiment mit 1.254 Teilnehmenden in Deutschland durchgeführt. Dabei wurden der Kontext sowie die technische und rechtliche Ausgestaltung einer vorgeschlagenen Überwachungsmaßnahme für private Smartphones variiert. Die Ergebnisse zeigen, dass die Unterstützung für Überwachungsmaßnahmen im Kontext von Terrorismus höher ist als im Kontext von Wohnungseinbruchsdiebstahl oder Gewaltverbrechen. Darüber hinaus führt eine Beschränkung der Massenüberwachungstauglichkeit sowie der durch die Überwachungsmaßnahme erhobenen Daten zu einer höheren Unterstützung für die Maßnahme. Ebenfalls zu einer höheren Unterstützung führt eine verpflichtende gerichtliche Anordnung der Maßnahme. Die Ergebnisse deuten somit auf eine hohe Relevanz der technischen und rechtlichen Ausgestaltung der Maßnahmen für die gesellschaftliche Akzeptanz hin.

1. Einleitung

Unter dem Eindruck verschiedener sich gegenseitig überlagernder und gegenseitig bedingender Krisen und Krisenerzählungen erleben wir aktuell wieder verstärkte Diskussionen über die öffentliche Sicherheit (Perkowski/Epik 2024). Der allgemeine Trend zur Digitalisierung macht dabei auch vor der Kommunikationsüberwachung nicht halt. Auf der einen Seite steht der Wunsch der Sicherheitsbehörden nach mehr Möglichkeiten der Überwachung digitaler Kommunikation, um auf die zunehmende Verschiebung

von Kommunikation in den digitalen Raum zu reagieren. Auf der anderen Seite besteht die Sorge vor zu großen staatlichen Eingriffen in die Privatsphäre der Bürger:innen, die in der Angst vor einem „Überwachungsstaat“ (Lüdemann/Schlepper 2013) Ausdruck findet.

In einem demokratischen Staat ist es jedoch auch wichtig, dass staatliche Maßnahmen von den Bürger:innen angenommen, mitgetragen und akzeptiert werden (Lüdemann/Schlepper 2011, S. 119). Der vorliegende Beitrag untersucht daher die gesellschaftlichen Einstellungen gegenüber staatlichen Überwachungsmaßnahmen. Da Einstellungen gegenüber der Privatsphäre und staatlichen Maßnahmen, die diese potenziell einschränken, stark kontextabhängig sind (Wright u. a. 2009, S. 69), wurden die Einstellungen in der Befragung, die in diesem Beitrag vorgestellt wird, mithilfe eines faktoriellen Survey-Experiments erhoben. Das Experiment erlaubte es, den Kontext der Maßnahme sowie die technische und rechtliche Ausgestaltung der Maßnahme kontrolliert zu variieren und so den Einfluss auf die Einstellung der Befragten zu untersuchen.

Als gesellschaftliche Akzeptanz bezeichnen wir in diesem Beitrag die positive bzw. negative Einstellung der Bevölkerung gegenüber bestimmten Überwachungsmaßnahmen (Petermann/Scherz 2005, S. 46f.). Dabei ist es uns wichtig festzuhalten, dass grundgesetzliche Wertungen nicht durch die Akzeptanzforschung ersetzt werden können und sollen. Die Erkenntnisse zur gesellschaftlichen Akzeptanz sollten vielmehr als Orientierung bei der Ausfüllung des verfassungsrechtlich vorgezeichneten Spielraums dienen. Ziel des Beitrags ist deshalb auch explizit nicht, die „Grenzen des (gerade noch) Akzeptablen“ (Kühne 2019, S. 38) auszuloten, um die Einführung gerade noch akzeptabler Überwachungsmaßnahmen zu unterstützen. Vielmehr geht es uns darum, ein differenziertes Bild der Akzeptanz in der deutschen Gesellschaft zu zeichnen und dabei den Blick auf die konkrete rechtliche und technische Ausgestaltung der Maßnahmen zu richten. Dies ist nur durch eine interdisziplinäre Betrachtungsweise möglich. Aus diesem Grund wurden Perspektiven aus den Bereichen Informatik, Jura und Soziologie in die Gestaltung des Experiments einbezogen.

Die Ergebnisse des Survey-Experiments zeigen: die Massenüberwachungstauglichkeit einer Maßnahme und die Intensität des Eingriffs in die Privatsphäre haben einen signifikanten Einfluss auf die Akzeptanz der Maßnahme. Ebenfalls einen signifikanten Einfluss auf die Akzeptanz von Überwachungsmaßnahmen haben die richterliche Kontrolle bei der Anwendung der Maßnahme und der zugrundeliegende Straftatbestand. Wie die Überwachung und damit der Zugang zu einem Gerät jedoch technisch

realisiert wird und ob dabei künstliche Intelligenz zum Einsatz kommt, zeigt im Experiment keine Auswirkung auf die Akzeptanz der Maßnahme.

2. Überwachung und Privatheit – konzeptuelle Fundierung

Überwachung kann viele Formen annehmen und es existiert eine Vielzahl unterschiedlicher Definitionen dieses Phänomens. Für diesen Beitrag übernehmen wir die Definition von Überwachung als „einseitige systematische, routinemäßige Beobachtung von Einzelpersonen oder Gruppen zu einem bestimmten Zweck“ (Trüdinger/Steckermeier 2017, S. 421). Moderne Überwachungstechnologien können ohne Zustimmung oder Wissen der Betroffenen personenbezogene Daten von Einzelpersonen extrahieren (Marx 2015). Dies kann durch die Nutzung öffentlich zugänglicher Informationen, die Überwachung öffentlicher Räume, zum Beispiel durch Kameras, oder den technischen Zugriff auf die Daten oder Geräte der Überwachten erfolgen. Überwachung kann darüber hinaus von verschiedenen Akteur:innen ausgehen. Neben privaten Akteur:innen, geht Überwachung vor allem von staatlichen Akteur:innen aus, die Überwachungsmaßnahmen unter anderem als strategisches Mittel zur Informationsbeschaffung einsetzen (Trüdinger/Steckermeier 2017, S. 421). Dieser Beitrag fokussiert sich vor allem auf Telekommunikationsüberwachung, eine Form der Überwachung, die Maßnahmen zur Überwachung von privaten Nachrichtenübermittlungen mittels technischer Einrichtungen umfasst (Zdun 2006, S. 325).

Privatheit ist ebenfalls ein facettenreiches Phänomen, von dem in verschiedenen Disziplinen verschiedenste Definitionen existieren (Möller u. a. 2025). Das Grundgesetz definiert die Privatsphäre nicht ausdrücklich als Rechtsbegriff. Auch der hiervon zu unterscheidende Begriff der Privatheit verfügt rechtlich über keine einheitliche Definition. Aspekte der Privatheit sind z. B. in Art. 10 GG, Art. 13 GG und in beinahe jedem Grundrecht enthalten (Heckmann, in: Stern u. a. 2022; Geminn/Roßnagel 2015, S. 703). Ausdrücklich findet sich die Achtung der Privatheit im Unionsrecht in Art. 7 GRCh.

Finn u. a. (2012, S. 7ff.) identifizieren sieben Typen von Privatheit. Von diesen sieben Typen ist für diesen Artikel vor allem der Typ „Privatheit von Kommunikation“ relevant. Privatheit von Kommunikation ist für eine demokratische Gesellschaft essenziell, da sie die Grundlage für eine freie Diskussionskultur bildet (Greenwald 2014). Gerade deshalb sind Einstellungen von Bürger:innen gegenüber Überwachungsmaßnahmen auch in Demo-

kratien von besonderer Relevanz und bereits Gegenstand verschiedener Studien (z. B. Davis/Silver 2004; Hallinan u. a. 2012; Lüdemann/Schlepper 2013). Allerdings behandeln viele Studien Überwachung als ein abstraktes Konzept und reduzieren die Einstellung dazu auf einen Wertekonflikt zwischen Freiheit und Sicherheit (z. B. Davis/Silver 2004; Jäger 2023). Die Studien nehmen dabei an, dass Bürger:innen rational die erwarteten Sicherheitsgewinne gegen die erwarteten Freiheits- und Privatheitseinschränkungen abwägen. Diese Annahme spiegelt sich oft auch im Studiendesign wider, in dem Befragte gebeten werden, ihre Präferenz zwischen Freiheit und Sicherheit anzugeben (Davis/Silver 2004).

Dabei wird davon ausgegangen, dass Bürger:innen den Zusammenhang zwischen Freiheit und Sicherheit als Nullsummenspiel verstehen. Studien zeigen allerdings, dass dies nicht der Fall ist. Die meisten Bürger:innen erwarten von ihren Regierungen, dass Überwachungsmaßnahmen so gestaltet sind, dass sie sowohl die Sicherheit erhöhen als auch die Privatsphäre schützen (Friedewald u. a. 2014; Pavone/Degli Esposti 2012). Daher ist es wichtig zu verstehen, wie staatliche Überwachungsmaßnahmen ausgestaltet und kontrolliert werden können, um potenzielle Risiken für die Privatsphäre möglichst zu minimieren, und wie sich diese Ausgestaltung auf die gesellschaftliche Einstellung gegenüber den Maßnahmen auswirkt.

3. Überwachungsmaßnahmen und Einstellung: Forschungsstand und Hypothesen

Ein weiterer Kritikpunkt an der Einstellungsforschung zu Überwachung als abstraktes Konzept ist, dass der Kontext, in dem die Überwachungsmaßnahme stattfindet, häufig ignoriert wird (Degli Esposti u. a. 2021; Wright u. a. 2009). Dabei wird vernachlässigt, dass Einstellungen gegenüber Überwachungsmaßnahmen nicht einfach existent sind, sondern Ausdruck der Interaktion zwischen Bürger:innen und sozialen und institutionellen Kontexten (Dourish/Anderson 2006).

Es ist daher unwahrscheinlich, dass alle Bürger:innen eine generelle Einstellung gegenüber allen staatlichen Überwachungsmaßnahmen entwickeln. Sie können eine bestimmte Überwachungsmaßnahme in einem bestimmten Kontext für gerechtfertigt halten, während sie eine andere Überwachungsmaßnahme im selben Kontext oder dieselbe Überwachungsmaßnahme in einem anderen Kontext ablehnen würden. Eine Möglichkeit diesen Umstand zu beforschen, ist der Vergleich von Einstellungen gegen-

über unterschiedlichen Überwachungstechnologien wie zum Beispiel Videoüberwachung und Online-Überwachung (Antoine 2023; Van den Broek u. a. 2017). Dabei wird allerdings außer Acht gelassen, dass diese Technologien unterschiedlich ausgestaltet sein können. Diese Ausgestaltungen könnten einen großen Einfluss auf die potenzielle Bedrohung der Privatheit und damit auch auf die Akzeptanz der Bevölkerung haben. Ein Video-Überwachungssystem kann beispielsweise Aufnahmen nur live übertragen oder sie auch speichern, zudem könnte automatisierte Gesichtserkennung zum Einsatz kommen (Li 2024).

Welchen Einfluss der jeweilige Kontext und die Ausgestaltung einer Überwachungsmaßnahme auf die Einstellung der Bürger:innen hat, soll daher in diesem Beitrag anhand der staatlichen Telekommunikationsüberwachung überprüft werden. Telekommunikation genießt sowohl nach dem Grundgesetz gemäß Art. 10 GG als auch nach der Grundrechtecharta der Union gemäß Art. 7 GRCh einen besonderen Schutz. Nach der jüngeren Rechtsprechung des Bundesverfassungsgerichts ist zudem, wenn zur Erfassung von Kommunikation ein Eingriff in das Endgerät erfolgt, auch das IT-System-Grundrecht gemäß Art. 2 Abs. 1 GG i. V. m. Art. 1 Abs. 1 GG einschlägig (BVerfG, Beschluss vom 24.06.2025 – 1 BvR 2466/19).

Einstellungen zu Privatheit und Maßnahmen, die diese potenziell einschränken, sind stark kontextabhängig (Wright u. a. 2009). Zum Kontext der Maßnahme gehört unter anderem der Grund, aus welchem die Maßnahme durchgeführt werden soll. Er stellt gewissermaßen den staatlichen Anlass für Eingriffe in die Privatsphäre dar (vgl. Lyon 2007). In der Debatte um staatliche Überwachungsmaßnahmen werden verschiedene Gründe angeführt. Während infolge der Terroranschläge des 11. September 2001 die Notwendigkeit von (weiteren) staatlichen Überwachungsmaßnahmen mit dem Schutz vor terroristischen Aktivitäten begründet wurde (Lyon/Haggerty 2012), spielt in der aktuellen Debatte auch der Schutz vor (organisierter) Kriminalität eine Rolle (Gruber u. a. 2022).

Diese unterschiedlichen Kontexte spiegeln sich auch in der Forschung wider. Die meisten Studien beforschen die Einstellungen zu staatlichen Überwachungsmaßnahmen allerdings nur in einem der beiden Kontexte, entweder im Kontext von Terrorismus (Garcia/Geva 2016; Trüdinger/Ziller 2022; Ziller/Helbling 2021) oder Kriminalität (Antoine 2023). Dabei wird der Effekt des Kontextes meist nicht direkt ermittelt oder adressiert. Eine Studie von Mondak und Hurwitz (2012) verglich die beiden Kontexte und untersuchte dabei nicht die Einstellung gegenüber Überwachung, sondern gegenüber anderen Maßnahmen, die die bürgerlichen Freiheiten

einschränken, wie beispielsweise Hausdurchsuchungen. Die Autoren stellten fest, dass der Kontext der Maßnahme einen messbaren Effekt auf die Zustimmung hat, die Maßnahmen im Zusammenhang mit Terrorismus erhielten eine höhere Zustimmung. Es ist plausibel anzunehmen, dass dieser Effekt bei Einstellungen zur Überwachung ebenfalls auftritt. Es ist allerdings auch möglich, dass Bürger:innen Überwachungsmaßnahmen im Kontext der Kriminalitätsbekämpfung eher akzeptieren, da die Wahrscheinlichkeit, selbst von Kriminalität betroffen zu sein und somit auch der potenzielle persönliche Nutzen für die eigene Sicherheit deutlich größer ist. Dies führt zu zwei möglichen Hypothesen:

H1a: Die Nutzung staatlicher Überwachung zur Bekämpfung von Terrorismus führt zu einer höheren Akzeptanz.

H1b: Die Nutzung staatlicher Überwachung zur Bekämpfung von Kriminalität führt zu einer höheren Akzeptanz.

Neben dem Kontext bestimmt die Ausgestaltung von Überwachungsmaßnahmen maßgeblich die potenzielle Gefahr, die von den Maßnahmen auf die Privatheit ausgeht. Frühere Studien zur Einstellung gegenüber staatlicher Überwachung identifizieren zwei Aspekte der Ausgestaltung, die die Einstellung der Öffentlichkeit gegenüber diesen Technologien stark beeinflussen: die Reichweite der Maßnahme und die Tiefe des Eingriffs in die Privatsphäre. Auch im Verfassungsrecht werden die Art und der Umfang der Datenerhebung als vertiefende Aspekte eines Grundrechtseingriffs berücksichtigt (BVerfG, Beschluss vom 24.06.2025 – 1 BvR 180/23, Rn. 187). Gleiches gilt für eine große Streubreite von Maßnahmen (BVerfGE 154, 152).

Je mehr Menschen potenziell von einer Überwachungsmaßnahme betroffen sind, desto größer ist die Gefahr anlassloser Massenüberwachung. Die Reichweite einer Überwachungsmaßnahme – gemessen als Anteil der davon betroffenen Bevölkerung – hat nachweislich einen erheblichen Einfluss auf die Einstellung gegenüber dieser Maßnahme: Während gezielte Maßnahmen, die sich gegen bestimmte Verdächtige richten, positiver bewertet werden, zeigt sich für Überwachungsmaßnahmen, die große Teile der Bevölkerung betreffen, weniger Akzeptanz (Antoine 2023; Jäger 2023; Ziller/Helbling 2021). Dies deckt sich mit den hohen verfassungsrechtlichen Hürden, welche von der Rechtsprechung an anlasslose Maßnahmen von hoher Streubreite gestellt werden (BVerfGE 154, 152, Rn. 168ff.; BVerfGE 125, 260, 320f.; differenzierend EuGH, Urteil vom 30.04.2024 – C-470/21). Unsere zweite Hypothese lautet daher:

H2: Eine Beschränkung der Reichweite der Maßnahme führt zu einer größeren Akzeptanz.

Abhängig davon, welche Daten bei einer Überwachungsmaßnahme erfasst werden, kann aus verfassungsrechtlicher Perspektive die Tiefe des mit der Maßnahme verbundenen Grundrechtseingriffs variieren. Der Eingriff in die Privatsphäre ist bei staatlicher Überwachung notwendig, da Überwachungsmaßnahmen explizit zum Ziel haben, Informationen über die Absichten und Pläne von Kriminellen oder Terrorist:innen zu ermitteln. Trotzdem obliegt es den staatlichen Stellen, den Eingriff in die Privatsphäre auf ein notwendiges Mindestmaß zu begrenzen. Dies ergibt sich aus dem Verhältnismäßigkeitsgrundsatz des Verfassungsrechts bei Grundrechtseingriffen. Vorangegangene Studien zeigten einen Zusammenhang zwischen der Sensibilität der bei der Überwachung erhobenen Daten und der öffentlichen Einstellung. So ist die öffentliche Akzeptanz für die Erfassung von Adressdaten höher als für die Überwachung von Internetnutzungsdaten (Antoine 2023). Unsere dritte Hypothese lautet daher:

H3: Eine Begrenzung des Ausmaßes der Eingriffe in die Privatsphäre führt zu einer höheren Akzeptanz.

Bürger:innen bilden ihre Einstellungen gegenüber staatlichen Überwachungsmaßnahmen in einem Kontext der Unsicherheit. Sie können den Einsatz der Maßnahme und die daraus resultierenden Auswirkungen nicht direkt kontrollieren. Dies gilt im Prinzip für jede Form des staatlichen Handelns, besonders aber für Überwachungsmaßnahmen, da diese oft verdeckt erfolgen und sich der Kontrolle damit aktiv entziehen (Trüdinger/Steckermeier 2017). Gleichzeitig sind die möglichen Konsequenzen, die sich aus einer Gefährdung der Privatheit bei einer missbräuchlichen Verwendung durch staatliche Stellen ergeben, besonders schwerwiegend, da diese meist über erhebliche Ressourcen verfügen. Folglich sind die Bürger:innen auf Dritte angewiesen, die die Anwendung von Überwachungsmaßnahmen in ihrem Namen kontrollieren. In einem demokratischen System sind die anderen Staatsgewalten für die Kontrolle der Exekutive zuständig. In diesem Zusammenhang nimmt die Justiz in Form der richterlichen Kontrolle eine Sonderstellung ein (Finn u. a. 2012, S. 8).

Pavone und Degli Esposti (2012) zeigten in einer qualitativen Studie mit spanischen Teilnehmenden, dass Bürger:innen die richterliche Kontrolle von Überwachungsmaßnahmen erwarten und in die Bewertung der Maßnahmen mit einbeziehen (Pavone/Degli Esposti 2012). Reddick und andere

(2015) zeigten außerdem in einer quantitativen Befragung in den USA, dass Bürger:innen, die davon ausgehen, dass Gerichte angemessene Grenzen für staatliche Überwachung setzen, eher dazu neigten, die staatlichen Überwachungsmaßnahmen zu billigen. Dies führt zu unserer vierten Hypothese:

H4: Die Notwendigkeit einer richterlichen Anordnung zur Durchführung der Überwachungsmaßnahme führt zu einer höheren Akzeptanz.

Die zunehmende Nutzung von Ende-zu-Ende-verschlüsselter digitaler Kommunikation stellt staatliche Behörden heutzutage vor große Probleme, denn klassische Telekommunikationsüberwachungsmaßnahmen, die die Kommunikation „von der Leitung“ abgreifen, können aus dem verschlüsselten Datenstrom kaum nützliche Informationen ableiten. Neuere Telekommunikationsüberwachungsmaßnahmen, wie etwa die Quellen-Telekommunikationsüberwachung oder die Online-Durchsuchung, funktionieren jedoch nur dann, wenn es den Behörden gelingt, eine (oft als Staatstrojaner bezeichnete) Software auf den verwendeten Endgeräten der Benutzer:innen auszuführen. Die Einbringung einer solchen Software gestaltet sich in der Praxis, beispielsweise aufgrund des hohen Sicherheitsniveaus moderner Smartphones, als schwierig. In der Praxis werden hierfür derzeit häufig nicht behobene Software-Sicherheitslücken genutzt, um Staatstrojaner zu installieren (Lawall/Scharping 2024, S. 606). Diese Praxis stellt ein erhebliches Risiko für andere Nutzende dar, da Kriminelle die nicht behobenen Software-Sicherheitslücken ebenfalls ausnutzen könnten (Vettermann u. a. 2023, S. 7). Behörden stehen daher vor dem Dilemma, die Öffentlichkeit durch die Schließung solcher Sicherheitslücken zu schützen und gleichzeitig den Fernzugriff für strafrechtliche Ermittlungen zu ermöglichen. Ein weiteres Problem betrifft den Erwerb von Kenntnissen über Schwachstellen. Dies führt häufig dazu, dass Regierungsbehörden an einem kriminellen Markt teilnehmen, auf dem diese Schwachstellen gehandelt werden (Lindenmeier u. a. 2024a, S. 27:2).

Zuletzt wurden jedoch neue technische Ansätze für den Zugriff auf Endgeräte vorgeschlagen, die eine an die klassische Telekommunikationsüberwachung angelehnte Mitwirkung der Softwareherstellenden vorsehen (Lindenmeier u. a. 2024a; 2024b). Da die Nutzung nicht behobener Software-Schwachstellen Risiken für die Öffentlichkeit mit sich bringt, ist zu erwarten, dass diese Praxis die öffentliche Akzeptanz verringern wird. Dies führt zur fünften Hypothese:

H5: Die Nutzung von nicht behobenen Software-Sicherheitslücken führt zu einer niedrigeren Akzeptanz.

Die rasanten Fortschritte in den Bereichen künstliche Intelligenz (KI) und maschinelles Lernen wirken sich auf fast alle Bereiche der Technologie aus. Überwachungstechnologien bilden dabei keine Ausnahme. KI-Systeme sind dabei vor allem im Bereich der automatisierten Datenauswertung relevant, da digitale Überwachungssysteme große Datenmengen produzieren. KI-Systeme könnten theoretisch aber auch genutzt werden, um die Privatsphäre der Betroffenen zu schützen, indem beispielsweise besonders schützenswerte Inhalte, die nicht mit dem Straftatbestand in Verbindung stehen, durch eine KI ausgefiltert werden, bevor ein Mensch die Daten zu Gesicht bekommt (Gleizer 2020).

Da die großen Fortschritte im Bereich von KI erst verhältnismäßig kurz zurückliegen, gibt es noch wenige Untersuchungen zu den möglichen Auswirkungen auf die Einstellung gegenüber Überwachungsmaßnahmen. Die wenigen vorliegenden Befunde sind dabei uneinheitlich. Nur eine Minderheit der deutschen Befragten steht dem Einsatz von KI durch Sicherheitsbehörden positiv gegenüber, die Tendenz ist jedoch steigend (Marcinkowski u. a. 2026). Eine Studie zur Akzeptanz von Videoüberwachung im Kontext von öffentlichem Nahverkehr stellte fest, dass die Befragten fortschrittlichere Kamertechnologien mit Echtzeit-Gesichtserkennung bevorzugen (Patil u. a. 2014). Andere Studien haben jedoch gezeigt, dass der Kontext und der Ort der Überwachung einen starken Einfluss auf die Einstellungen haben. Die Akzeptanz von Überwachung ist im öffentlichen Raum größer (Van Heek u. a. 2017). Es ist daher unklar, ob diese Ergebnisse auf den Kontext der Überwachung privater Telekommunikation übertragbar sind.

Ein weiteres Argument, das vor allem von Mitarbeiter:innen staatlicher Behörden vorgebracht wird, lautet, dass Betroffene die Überwachung als weniger invasiv empfinden, wenn personenbezogene Daten nicht von einem Menschen eingesehen, sondern automatisch von einer Maschine analysiert werden (Cayford/Pieters 2018, S. 97; Moll/Schneider 2021, S. 102).

Diese Befunde führen zu drei alternativen Hypothesen:

H6a: Der Einsatz künstlicher Intelligenz in Überwachungsmaßnahmen führt generell zu einer geringeren Akzeptanz.

H6b: Der Einsatz künstlicher Intelligenz in Überwachungsmaßnahmen führt generell zu einer höheren Akzeptanz.

H6c: Der Einsatz künstlicher Intelligenz in Überwachungsmaßnahmen führt nur dann zu einer größeren öffentlichen Akzeptanz, wenn durch den Einsatz von künstlicher Intelligenz die Privatsphäre der Betroffenen geschützt werden soll.

4. Datenbasis und methodisches Vorgehen

Um die aufgestellten Hypothesen empirisch zu überprüfen, wurde im Februar und März 2025 in Deutschland ein faktorielles Survey-Experiment durchgeführt. Bei diesem wurden den Befragten verschiedene Versionen einer möglichen Überwachungsmaßnahme präsentiert. Dabei wurden bestimmte Abschnitte des Textes, welche die rechtliche und technische Ausgestaltung der Maßnahme beschreiben, experimentell variiert. Die einzelnen Versionen des Beschreibungstexts werden als „Vignetten“ bezeichnet. Anschließend gaben die Befragten ihre Zustimmung zu der Maßnahme an. Dies erlaubt uns, den Einfluss der rechtlichen und technischen Ausgestaltung auf die Zustimmung zu messen (Auspurg/Hinz 2015). Die Befragung wurde mit Hilfe eines Online-Access Panel Anbieters (Norstat) realisiert. Bei der Kontaktierung der Befragten wurden Quoten für Alter, Geschlecht und Bildung eingesetzt. Die Stichprobe entspricht hinsichtlich der Verteilung dieser Merkmale der deutschen Gesamtbevölkerung. Insgesamt haben 1.254 Personen an der Umfrage teilgenommen.

Im vorherigen Abschnitt haben wir argumentiert, dass die Einstellung gegenüber staatlichen Überwachungsmaßnahmen in der Bewertung einer komplexen Situation entsteht, in der soziale und institutionelle Kontexte eine Rolle spielen (Wright u. a. 2009). Wenn sich Bürger:innen eine Meinung zu einer bestimmten Überwachungsmaßnahme bilden, müssen sie verschiedene Faktoren abwägen. Dazu gehören die Art, Leistungsfähigkeit und Eingriffstiefe der eingesetzten Technologie und die daraus resultierenden Gefahren für die Privatsphäre sowie die Gründe für die Überwachungsmaßnahme.

Um diese Abwägung für die Befragten greifbar zu machen, erfassen wir ihre Einstellungen anhand des konkreten Beispiels der polizeilichen Überwachung privater Smartphones. Die Überwachung privater Endgeräte kann dabei als „least-likely case“ für die Akzeptanz der Maßnahme angesehen werden. Vorangegangene Studien zeigen zum einen, dass heimliche Überwachung im privaten Raum deutlich stärker abgelehnt wird als die sichtbare Überwachung öffentlicher Räume (Pavone/Degli Esposti 2012;

Van den Broek u. a. 2017; Ziller/Helbling 2021). Konsequenterweise stellte Trüdinger (2018) in einer repräsentativen Umfrage fest, dass die Überwachung privater Telekommunikation die am wenigsten unterstützte staatliche Überwachungsmaßnahme in der deutschen Bevölkerung darstellt. Wenn Bürger:innen also bereit sind, staatliche Maßnahmen zur Überwachung privater Telekommunikation unter bestimmten Bedingungen zu unterstützen, ist es wahrscheinlich, dass diese Bedingungen auch bei weniger privatsphäreintensiven Eingriffen zu einer höheren Akzeptanz führen könnten.

Bei der Befragung kam ein vollfaktorielles Survey-Experiment ($3 \times 2 \times 2 \times 2 \times 3 \times 2$) (Auspurg/Hinz 2015) zum Einsatz. Aus den einzelnen Dimensionen des Experiments wurden 144 einzigartige Vignettentexte erstellt. In diesen Vignettentexten wurde ein hypothetisches Gesetz beschrieben, das den Einsatz einer Überwachungsmaßnahme vorsieht. Im Anschluss konnten die Befragten auf einer siebenstufigen Likert-Skala angeben, ob sie das Gesetz eher unterstützen oder ablehnen. Die Befragten erhielten zufällig drei der 144 Vignetten zur Bewertung, was zu einer Anzahl von 3.762 bewerteten Vignetten führte. Aufgrund fehlender Werte können nur 3.760 der bewerteten Vignetten in der folgenden Analyse verwendet werden.

Tabelle 1: Dimensionen und Level des Experiments

Dimension	Level 1	Level 2	Level 3
Kontext	Zur Bekämpfung von Terrorismus	Zur Bekämpfung von Gewaltverbrechen	Zur Bekämpfung von Wohnungseinbruchdiebstahl
Reichweite	Technisch wäre es möglich mit der Überwachungsmaßnahme große Teile der Bevölkerung zu überwachen	Die Überwachungsmaßnahme wird technisch so beschränkt, dass eine massenhafte Überwachung von großen Teilen der Bevölkerung nicht möglich ist	
Ausmaß Eingriff Privatsphäre	Nachrichten von Messengerdiensten (z.B. WhatsApp, Telegram, Signal) einzusehen	auf alle Inhalte eines Smartphones (z.B. Fotos, Videos & Textnachrichten) zuzugreifen	
Richterliche Anordnung	Für den Einsatz der Software ist ein richterlicher Beschluss notwendig	Für den Einsatz der Software ist kein richterlicher Beschluss notwendig	

Dimension	Level 1	Level 2	Level 3
Ausnutzung Software Schwachstellen	Dabei werden technische Schwachstellen genutzt, die auch von Kriminellen ausgenutzt werden könnten	Dabei werden die Hersteller der Smartphones zur Zusammenarbeit mit der Polizei verpflichtet.	
KI-Einsatz	Um die Ergebnisse der Auswertung zu verbessern, soll künstliche Intelligenz eingesetzt werden	Mithilfe von künstlicher Intelligenz sollen private Inhalte aussortiert werden, bevor ein Mensch die Daten betrachtet	Keine Angabe

Die Details der Überwachungsmaßnahme werden experimentell über sechs Dimensionen hinweg variiert (s. Tab. 1). Die Dimensionen umfassen den strafrechtlichen Kontext der Maßnahme (Kriminalität vs. Terrorismus), die Reichweite in Form der Massenüberwachungstauglichkeit der Maßnahme, das Ausmaß des Eingriffes in die Privatsphäre, die Notwendigkeit einer richterlichen Anordnung der Maßnahme, die Ausnutzung von Schwachstellen für den Zugriff sowie den Einsatz von künstlicher Intelligenz. Der folgende Absatz enthält ein Beispiel für eine Vignette, wobei die manipulierten Dimensionen kursiv hervorgehoben sind.

Zur Bekämpfung von *Gewaltverbrechen* soll ein Gesetz verabschiedet werden, das der Polizei ermöglicht *Nachrichten von Messengerdiensten (z. B. WhatsApp, Telegram, Signal) einzusehen*. Dabei werden *die Hersteller der Smartphones zur Zusammenarbeit mit der Polizei verpflichtet*. Technisch wäre es möglich, mit der Überwachungsmaßnahme *große Teile der Bevölkerung zu überwachen*. *Mithilfe von künstlicher Intelligenz sollen private Inhalte aussortiert werden, bevor ein Mensch die Daten betrachtet*. Für den Einsatz der Software ist *ein richterlicher Beschluss* notwendig.

Im Folgenden gehen wir näher auf die einzelnen Dimensionen ein, die im Experiment manipuliert werden. Jede Dimension kann bis zu drei Ausprägungen annehmen. Bei der ersten Dimension handelt es sich um den Kontext der Maßnahme. Neben dem Unterschied zwischen Terrorismus und Alltagskriminalität interessieren wir uns außerdem dafür, welchen Einfluss die Verletzung der körperlichen Unversehrtheit auf die Zustimmung zur Maßnahme hat. Daher wurden im Experiment die Bekämpfung von Terrorismus, die Bekämpfung von Gewaltverbrechen und die Bekämpfung von Wohnungseinbruchsdiebstahl als Gründe für die Maßnahme genannt.

Die zweite und dritte Dimension beschreiben die technischen und rechtlichen Beschränkungen hinsichtlich der Reichweite und der Eingriffstiefe

der Überwachungsmaßnahme. Die Reichweite der Maßnahme wird durch die Eignung der Maßnahme zur Massenüberwachungstauglichkeit operationalisiert. Die Eingriffstiefe in die Privatsphäre wird anhand der Menge der von der Maßnahme betroffenen privaten Daten operationalisiert. Die erste Ausprägung beschreibt eine Situation, in der der Zugriff auf Kommunikation beschränkt ist. Dies entspricht den erhobenen Daten bei der Telekommunikationsüberwachung, zum Beispiel nach § 100a StPO. Die zweite Ausprägung beschreibt eine Situation, in der die Polizei Zugriff auf alle Informationen auf dem Gerät hat, einschließlich privater Daten, die nicht Teil eines Kommunikationsprozesses waren. Die erhobenen Daten in der zweiten Stufe entsprechen der Online-Durchsuchung, zum Beispiel nach § 100b StPO.

Die Ausnutzung von unbekannten Software-Schwachstellen zur Ermöglichung von staatlichen Maßnahmen wird vor allem deswegen kritisiert, weil dies in der Konsequenz dazu führt, dass diese Schwachstellen nicht sofort geschlossen werden, was möglicherweise durch Kriminelle ausgenutzt werden könnte (Klauser u. a. 2026). Da dieser Diskurs vermutlich nicht allen Befragten bekannt ist, wurde die mögliche Konsequenz dieser Praxis im Vignettentext erwähnt. Als Alternative zur Nutzung von Schwachstellen wird in der zweiten Ausprägung die Verpflichtung der Herstellenden zur Kooperation beim Zugang zum Gerät (Lindenmeier u. a. 2024a, S. 27:6) genannt.

Der Einsatz von KI wird über drei Ebenen variiert. Die erste Ausprägung beschreibt den Einsatz von KI mit dem Ziel, die Privatsphäre besser zu schützen. Dies soll dadurch erreicht werden, dass eine KI besonders sensible Daten, die nichts mit der polizeilichen Ermittlung zu tun haben, ausfiltert, bevor ein Mensch sie zu Gesicht bekommt. Die zweite Ausprägung beschreibt den Einsatz von KI zur Verbesserung der Datenauswertung. Zum Vergleich wird die Nutzung von KI in der dritten Ausprägung nicht erwähnt. Die letzte Dimension beschreibt, ob für die Durchführung der Überwachungsmaßnahme eine richterliche Anordnung erforderlich ist. Zur Überprüfung der aufgestellten Hypothesen wurde eine OLS-Regression mit clusterrobusten Standardfehlern auf Befragtenebene durchgeführt.

5. Ergebnisse

Von allen experimentellen Varianten der vorgeschlagenen Überwachungsmaßnahmen wurden 47,4% der Vignetten von den Befragten zustimmend

bewertet (Antworten über der mittleren Kategorie der siebenstufigen Antwortskala), während 32,5% ablehnend bewertet wurden. 20,1% der Vignetten erhielten unentschiedene Bewertungen in der mittleren Kategorie. Diese Zustimmungsrate entspricht den Ergebnissen anderer faktorieller Experimente zur Akzeptanz von Überwachungsmaßnahmen in Deutschland (Antoine 2023; Ziller/Helbling 2021).

Abb. 1 zeigt die Ergebnisse des faktoriellen Survey-Experiments. Auf der vertikalen Achse sind die Dimensionen des Experiments aufgeführt, darunter eingeschränkte Massenüberwachungstauglichkeit, eingeschränkter Datenzugriff, die Notwendigkeit eines richterlichen Beschlusses, Nutzung von Schwachstellen, Wohnungseinbruchdiebstahl, Gewaltverbrechen sowie KI zur Auswertung und KI zum Schutz der Privatsphäre. Auf der horizontalen Achse sind geschätzte Effekte relativ zu einer vertikalen gestrichelten Nulllinie dargestellt. Punkte mit Linien zeigen Effekte und Konfidenzintervalle. Effekte, bei denen das Konfidenzintervall nicht die Null-Linie schneidet, können als signifikant betrachtet werden. Das bedeutet, dass es unwahrscheinlich ist, dass die Effekte zufällig in der Stichprobe aufgetreten sind. Eingeschränkter Datenzugriff, eingeschränkte Massenüberwachungstauglichkeit und notwendiger richterlicher Beschluss weisen signifikant positive Effekte auf. Diese Dimensionen haben die Zustimmung zur Maßnahme signifikant erhöht. Signifikant negative Effekte zeigen hingegen Wohnungseinbruchdiebstahl und Gewaltverbrechen im Vergleich zur Referenzkategorie Terrorismus. Daraus lässt sich ableiten, dass die Zustimmung zur Maßnahme bei der Präsentation der Maßnahme im Kontext der beiden genannten Verbrechen signifikant niedriger war als im Kontext von Terrorismus. Die Effekte für die Nutzung von Schwachstellen und den Einsatz von KI sind eher klein und nicht signifikant, wir können uns daher nicht sicher sein, ob die Effekte durch Zufall in unserer Stichprobe entstanden sind.

Wenn der Kontext der vorgeschlagenen Überwachungsmaßnahme Kriminalität statt Terrorismus ist, ist die Akzeptanz der Maßnahme deutlich geringer (s. Abb. 1). Dies gilt für beide vorgestellten Straftaten: Einbruch und Gewaltverbrechen. Hypothese 1b muss daher verworfen werden (s. Tab. 2). Die Akzeptanz der Maßnahme ist zudem deutlich höher, wenn ihre Reichweite beschränkt ist. Dieses Ergebnis steht im Einklang mit Hypothese 2. Der gleiche Effekt tritt auch bei einer Begrenzung des Ausmaßes des Eingriffs in die Privatsphäre auf, was mit der dritten Hypothese übereinstimmt. Wie in Hypothese vier postuliert, erhöht die Notwendigkeit einer richterlichen Anordnung für den Einsatz der Überwachungsmaßnahme die

Akzeptanz deutlich. Die Nutzung von Software-Schwachstellen hat hingegen keinen signifikanten Einfluss auf die Akzeptanz. Die fünfte Hypothese konnte somit nicht bestätigt werden. Ebenfalls keinen signifikanten Einfluss hat der Einsatz von künstlicher Intelligenz. Weder zur Verbesserung des Schutzes der Privatsphäre noch zur Verbesserung der Auswertung. Die Hypothesen zur Nutzung von künstlicher Intelligenz konnten somit im Experiment ebenfalls nicht bestätigt werden.

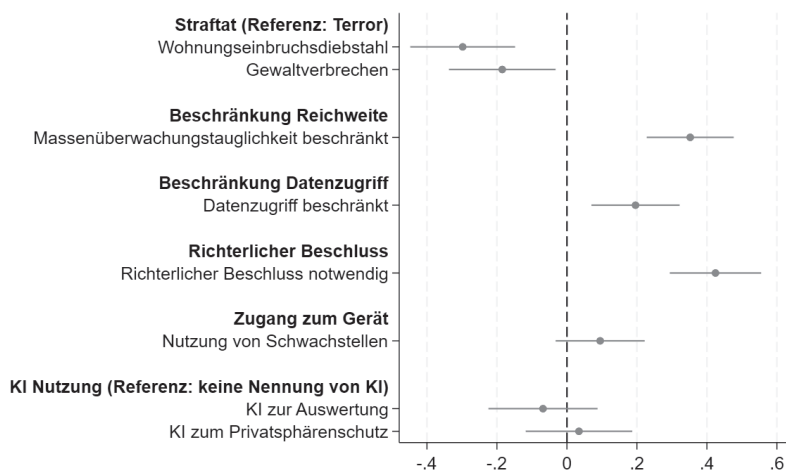


Abbildung 1: Regressionskoeffizienten mit 95%-Konfidenzintervallen

Zur Überprüfung der Robustheit der Ergebnisse wurde ein Regressionsmodell mit zusätzlichen Kontrollvariablen berechnet. In diesem Modell wurden Geschlecht, Alter, Haushaltseinkommen, Bildung, Region (Ost- oder Westdeutschland), Migrationshintergrund (ob die Person selbst oder ihre Eltern migriert sind) sowie die Zugehörigkeit zu einer religiösen Minderheit berücksichtigt. Alter hat in diesem Modell, unabhängig von der Ausgestaltung der Maßnahme, einen signifikanten positiven Einfluss auf die Akzeptanz. Dieses Ergebnis deckt sich mit anderen Studien zur Akzeptanz von Überwachungsmaßnahmen in Deutschland (Antoine 2023, S. 430; Bug/Bukow 2017, S. 203; Friedewald u. a. 2015, S. 70; Kostka u. a. 2023, S. 8). Das Haushaltseinkommen und der Bildungsstand haben, unabhängig von der Ausgestaltung der Maßnahme, einen signifikanten negativen Einfluss auf die Akzeptanz. Auch dieses Ergebnis stimmt mit der Literatur

überein (Friedewald u. a. 2015, S. 70; Trüdinger/Steckermeier 2017, S. 426). Trotz der signifikanten Effekte bei einigen der Kontrollvariablen weichen die Effekte der Vignetten-Dimensionen im Kontrollmodell nicht signifikant vom unkontrollierten Modell ab.

Tabelle 2: Ergebnisse der Hypothesenprüfung

Hypothesen	Unterstützung der Hypothese
H1a: Die Nutzung staatlicher Überwachung zur Bekämpfung von Terrorismus führt zu einer höheren Akzeptanz.	✓
H1b: Die Nutzung staatlicher Überwachung zur Bekämpfung von Kriminalität führt zu einer höheren Akzeptanz.	✗
H2: Eine Beschränkung der Reichweite der Maßnahme führt zu einer höheren Akzeptanz.	✓
H3: Eine Begrenzung des Ausmaßes der Eingriffe in die Privatsphäre führt zu einer höheren Akzeptanz.	✓
H4: Die Notwendigkeit einer richterlichen Anordnung zur Durchführung der Überwachungsmaßnahme führt zu einer höheren Akzeptanz.	✓
H5: Die Nutzung von nicht behobenen Software-Sicherheitslücken führt zu einer niedrigeren Akzeptanz.	✗
H6a: Der Einsatz künstlicher Intelligenz in Überwachungsmaßnahmen führt generell zu einer geringeren Akzeptanz.	✗
H6b: Der Einsatz künstlicher Intelligenz in Überwachungsmaßnahmen führt generell zu einer höheren Akzeptanz.	✗
H6c: Der Einsatz künstlicher Intelligenz in Überwachungsmaßnahmen führt nur dann zu einer größeren öffentlichen Akzeptanz, wenn durch den Einsatz von künstlicher Intelligenz die Privatsphäre der Betroffenen geschützt werden soll.	✗

6. Diskussion und Fazit

Das Hauptziel dieser Studie bestand darin, mithilfe eines faktoriellen Survey-Experiments festzustellen, wie der Kontext sowie die rechtliche und technische Ausgestaltung einer staatlichen Überwachungsmaßnahme die gesellschaftliche Akzeptanz der Maßnahme beeinflussen.

Im Kontext von Wohnungseinbruchsdiebstahl und Gewaltverbrechen ist die Zustimmung zu den vorgeschlagenen Überwachungsmaßnahmen deutlich geringer als im Kontext von Terrorismus. Da die Wahrscheinlichkeit, Opfer eines Einbruchs oder Gewaltverbrechens zu werden, deutlich höher ist als die Wahrscheinlichkeit, Opfer eines Terroranschlags zu werden, lässt

diese Erkenntnis den Schluss zu, dass die Befragten den Einsatz staatlicher Überwachung zur Bekämpfung gesellschaftlicher Bedrohungen für legitimer halten als zur Bekämpfung von Individualkriminalität. Dieses Ergebnis steht im Einklang mit den Ergebnissen von Mondak und Hurwitz (2012), die ebenfalls eine höhere Akzeptanz für Maßnahmen zur Einschränkung bürgerlicher Freiheiten im Zusammenhang mit Terrorismus feststellten.

Die Akzeptanz der Überwachungsmaßnahmen ist im Experiment deutlich höher, wenn die Massenüberwachungstauglichkeit begrenzt ist und der Eingriff in die Privatsphäre der Betroffenen gering ausfällt. Diese Ergebnisse stehen ebenfalls im Einklang mit vorhergegangenen Studien, die eine stärkere Akzeptanz gegenüber Überwachungsmaßnahmen feststellten, die sich gegen bestimmte Personen richten und nicht die gesamte Bevölkerung betreffen (Antoine 2023; Ziller/Helbling 2021). Die Ergebnisse bestätigen vorangegangene Studien, die eine geringere Akzeptanz von Überwachungsmaßnahmen mit einem größeren Potenzial für Eingriffe in die Privatsphäre feststellten (Antoine 2023).

Das Gleiche gilt für die institutionelle Kontrolle in Form richterlicher Anordnungen. Wenn diese Anordnungen für die Durchführung der Überwachungsmaßnahme erforderlich sind, steigt die Akzeptanz der Maßnahme deutlich an. Der Effekt der richterlichen Kontrolle ist der stärkste unter den manipulierten Variablen im Experiment. Dieses Ergebnis deckt sich mit den Forschungsergebnissen von Pavone und Degli Esposti (2012, S. 563), die die Wichtigkeit richterlicher Kontrolle für die Einstellungsbildung gegenüber staatlicher Überwachung in qualitativen Fokusgruppeninterviews in Spanien feststellten. Unsere Ergebnisse zeigen, dass der Effekt richterlicher Kontrolle vom spanischen auf den deutschen Kontext übertragbar ist und deuten deshalb darauf hin, dass die Aufsicht durch Gerichte und Richter eine wichtige Voraussetzung für die Akzeptanz von Überwachungsmaßnahmen in verschiedenen nationalen Kontexten ist. Die qualitativen Befunde der Fokusgruppeninterviews aus der Studie von Pavone und Degli Esposti (2012) konnten wir darüber hinaus in unserer Studie in einem quantitativen, bevölkerungsrepräsentativen Sample replizieren.

In unserem Experiment beschreiben wir eine Vorabkontrolle der Überwachungsmaßnahme durch einen Richter. In zeitkritischen Situationen kann auch eine Abweichung davon zulässig sein (§100e Abs. 1 Satz 2, 3 StPO). Für zukünftige Forschungsvorhaben könnte es von Interesse sein, zu ermitteln, inwiefern es bezüglich der Akzeptanz einen Unterschied macht, ob die Kontrolle vorab oder erst nachträglich erfolgt.

Die Frage, ob kritische Software-Schwachstellen zur Durchführung staatlicher Überwachungsmaßnahmen auf Smartphones genutzt werden sollten, ist ein zentrales Thema der deutschen Überwachungsdebatte (Freiling u. a. 2017; Rehak 2013; Vettermann u. a. 2023).

Überraschenderweise hat die Nennung der Nutzung von Schwachstellen im Experiment keine signifikante Wirkung im Vergleich zur Verpflichtung der Smartphone-Herstellenden zur Zusammenarbeit. Dafür gibt es mehrere mögliche Erklärungen. Die Debatte betrifft möglicherweise nur Expert:innen und findet in der Öffentlichkeit keinen Widerhall. Da das Problem der Software-Schwachstellen sehr technisch ist, ist es zudem möglich, dass einige Befragte den Inhalt dieser Dimension nicht verstanden haben. Eine alternative Erklärung ist, dass die Verpflichtung der Herstellenden zur Kooperation für die Befragten keine signifikant bessere Alternative darstellt, da auch dieses Vorgehen eine Reihe ungeklärter Probleme, wie die regelmäßige Involvierung einer Vielzahl von Herstellenden aus unterschiedlichen nationalen Kontexten zur Folge hätte (vgl. Klauser u. a. 2026). Vorangegangene Studien zeigen zudem, dass die Skepsis gegenüber privatwirtschaftlichen Akteur:innen im Kontext der Überwachung deutlich höher ist als gegenüber staatlichen Akteur:innen (Van den Broek u. a. 2017, S. 21f.). Dieser Umstand könnte ebenfalls dazu beitragen, dass die Befragten die Involvierung privater Herstellenden nicht stärker unterstützen als das Ausnutzen von Schwachstellen.

Trotz der gesellschaftlichen Debatte über den Einsatz künstlicher Intelligenz und die damit einhergehenden Gefahren (Ittefaq u. a. 2025) konnten wir in unserem Experiment keinen signifikanten Effekt durch die Nutzung von künstlicher Intelligenz feststellen. Dies gilt auch, wenn der Einsatz der künstlichen Intelligenz explizit zur Verbesserung des Schutzes der Privatsphäre verwendet werden soll. Das Argument, dass Befragte Überwachungsmaßnahmen positiver gegenüberstehen, wenn diese weitestgehend automatisiert und ohne menschliches Zutun ablaufen (Cayford/Pieters 2018, S. 97), konnte somit im Experiment nicht gestützt werden.

Insgesamt zeigen die Ergebnisse des Experiments, dass es sinnvoll ist, die gesellschaftlichen Einstellungen zu staatlichen Überwachungsmaßnahmen nicht abstrakt zu erfragen, sondern die konkrete Ausgestaltung der Maßnahmen mit zu berücksichtigen.

Grundsätzlich lässt sich feststellen, dass neben der Begrenzung der Maßnahme auf schwerste Straftaten wie Terrorismus vor allem die Dimensionen, die mit der Beschränkung und Kontrolle der Maßnahme zusammenhängen, einen Einfluss auf die Akzeptanz hatten. Dazu gehören die

Beschränkung der Massenüberwachungstauglichkeit und des Eingriffs in die Privatsphäre sowie die richterliche Kontrolle. Gleichzeitig haben die Dimensionen, die eher mit der technischen Umsetzung der Maßnahme zusammenhängen, wie die Nutzung von Schwachstellen für den Zugang zum Gerät und der Einsatz von künstlicher Intelligenz, keinen signifikanten Einfluss auf die Zustimmung zur Maßnahme. Für die Politikgestaltung lässt sich daraus ableiten, dass die Sicherstellung der Beschränkung und Kontrolle der Maßnahme für die gesellschaftliche Akzeptanz wichtiger ist als die technischen Details der Ausgestaltung.

Je nach gewähltem Ansatz weisen empirische Studien Stärken, aber auch Limitationen auf, die hinsichtlich der Interpretation und Generalisierbarkeit der Ergebnisse berücksichtigt werden müssen. Ein Vorteil des in dieser Studie gewählten Ansatzes ist, dass die detaillierte Beschreibung der technischen und rechtlichen Aspekte der vorgestellten Überwachungsmaßnahme eher dem alltäglichen politischen Diskurs entspricht, in dem bestimmte Maßnahmen öffentlich diskutiert werden.

Gleichzeitig besteht die Gefahr, dass genau dieser Detailreichtum bei den beschriebenen Maßnahmen für einige Befragte überwältigend sein könnte. Dies gilt insbesondere, wenn die Befragten ihre Einstellungen zur staatlichen Überwachung auf einer allgemeineren Ebene bilden. Daher sind weitere Untersuchungen erforderlich, um festzustellen, wie Überwachungsszenarien auf verschiedenen Abstraktionsebenen dargestellt werden sollten.

In dieser Studie wurden Einstellungen zur staatlichen Überwachung am Beispiel der Überwachung privater Kommunikationsgeräte untersucht. Die Frage, inwiefern sich die Ergebnisse auf andere Formen staatlicher Überwachung in anderen Kontexten, wie beispielsweise Videoüberwachung im öffentlichen Raum oder die Überwachung des privaten Surfverhaltens im Internet, übertragen lassen, bleibt offen. Hierzu ist weitere Forschung notwendig, die die Einstellungen gegenüber staatlichen Überwachungsmaßnahmen in Abhängigkeit von deren konkreter rechtlicher und technischer Ausgestaltung untersucht.

Danksagung

Dieser Beitrag entstand im Rahmen des SEpES-Projekts am bayerischen Forschungsinstitut für Digitale Transformation (bidt). Wir bedanken uns bei den Teilnehmenden der Jahreskonferenz der Plattform Privatheit 2025 für die wertvollen Anmerkungen. Für die Unterstützung bei der Formulierung und der Recherche bedanken wir uns bei unserer studentischen Hilfskraft Maj Britt Busch.

Literatur

- Antoine, Lukas (2023): Costs, Inconvenience, or Civil Rights? Investigating Determinants of Public Support for Surveillance. *Surveillance & Society*, 21(4), S. 409–431. <https://doi.org/10.24908/ss.v21i4.15796>
- Auspurg, Katrin und Hinz, Thomas (2015): *Factorial Survey Experiments*. Thousand Oaks: SAGE Publications. <https://doi.org/10.4135/9781483398075>
- Bug, Mathias und Bukow, Sebastian U. (2017): Civil Liberties vs. Security: Why Citizens Accept or Reject Digital Security Measures. *German Politics*, 26(2), S. 292–313. <https://doi.org/10.1080/09644008.2016.1226811>
- Cayford, Michelle und Pieters, Wolter (2018): The effectiveness of surveillance technology: What intelligence officials are saying. *The Information Society*, 34(2), S. 88–103. <https://doi.org/10.1080/01972243.2017.1414721>
- Davis, Darren W. und Silver, Brian D. (2004): Civil Liberties vs. Security: Public Opinion in the Context of the Terrorist Attacks on America. *American Journal of Political Science*, 48(1), S. 28–46. <https://doi.org/10.1111/j.0092-5853.2004.00054.x>
- Degli Esposti, Sara; Ball, Kirstie und Dibb, Sally (2021): What's In It For Us? Benevolence, National Security, and Digital Surveillance. *Public Administration Review*, 81(5), S. 862–873. <https://doi.org/10.1111/puar.13362>
- Dourish, Paul und Anderson, Ken (2006): Collective Information Practice: Exploring Privacy and Security as Social and Cultural Phenomena. *Human-Computer Interaction*, 21(3), S. 319–342. https://doi.org/10.1207/s15327051hci2103_2
- Finn, Rachel L.; Wright, David und Friedewald, Michael (2012): Seven types of privacy. In: Gutwirth, Serge; Leenes, Ronald; de Hert, Paul und Poulet, Yves (Hrsg.): *European data protection: Coming of age*. Dordrecht: Springer, S. 3–32.
- Freiling, Felix; Safferling, Christoph und Rückert, Christian (2017): Quellen-TKÜ und Online-Durchsuchung als neue Maßnahmen für die Strafverfolgung: Rechtliche und technische Herausforderungen. *Juristische Rundschau*, 1/2018, S. 9–22. <https://doi.org/10.1515/juru-2017-0104>
- Friedewald, Michael; van Lieshout, Marc; Rung, Sven; Ooms, Merel und Ypma, Jelmer (2014): Privacy and security perceptions of European citizens: A test of the trade-off model. In: Camenisch, Jan; Fischer-Hübner, Simone und Hansen, Marit (Hrsg.): *Privacy and Identity Management for the Future Internet in the Age of Globalisation. Privacy and Identity 2014. IFIP Advances in Information and Communication Technology*, vol. 457. Cham: Springer, S. 39–53.
- Friedewald, Michael; Rung, Sven; van Lieshout, Marc; Ooms, Merel; van der Broek, Tijs und Ypma, Jelmer (2015): Deliverable 10.1: Report on statistical analysis of the PRISMS survey. Brüssel: PRISMS Project (EU FP7, GA 285399). URL: <https://public.a.fraunhofer.de/handle/publica/297523> (besucht am 09.04.2026).
- Garcia, Blake E. und Geva, Nehemia (2016): Security Versus Liberty in the Context of Counterterrorism: An Experimental Approach. *Terrorism and Political Violence*, 28(1), S. 30–48. <https://doi.org/10.1080/09546553.2013.878704>
- Geminn, Christian und Roßnagel, Alexander (2015): „Privatheit“ und „Privatsphäre“ aus der Perspektive des Rechts—ein Überblick. *JuristenZeitung*, 14/2015, S. 703–708.

- Gleizer, Orlandino (2020): Algorithmischer Kernbereichsschutz. Zum Einsatz von künstlicher Intelligenz in der Online-Durchsuchung als Staatspflicht. In: Kusche, Carsten; Beck, Susanne und Valerius, Brian (Hrsg.): *Digitalisierung, Automatisierung, KI Und Recht*. Baden-Baden: Nomos, S. 535–556.
- Greenwald, Glenn (2014): *No place to hide: Edward Snowden, the NSA, and the US surveillance state*. New York: Metropolitan Books.
- Gruber, Jan; Brodowski, Dominik und Freiling, Felix (2022): Die polizeiliche Aufgabe und Pflicht zur digitalen Gefahrenabwehr. *Zeitschrift Für Das Gesamte Sicherheitsrecht*, 4/2022, S. 171–176.
- Hallinan, Dara; Friedewald, Michael und McCarthy, Paul (2012): Citizens' perceptions of data protection and privacy in Europe. *Computer Law & Security Review*, 28(3), S. 263–272. <https://doi.org/10.1016/j.clsr.2012.03.005>
- Heckmann, Dirk (2022): Schutz von Persönlichkeit und Privatsphäre. In: Stern, Klaus; Sodan, Helge und Möstl, Markus (Hrsg.): *Das Staatsrecht der Bundesrepublik Deutschland im europäischen Staatenverbund*. München: C. H. Beck, S. 108–122.
- Ittefaq, Muhammad; Zain, Ali; Arif, Rauf; Ala-Uddin, Mohammad; Ahmad, Taufiq und Iqbal, Azhar (2025): Global news media coverage of artificial intelligence (AI): A comparative analysis of frames, sentiments, and trends across 12 countries. *Telematics and Informatics*, 96, 102223. <https://doi.org/10.1016/j.tele.2024.102223>
- Jäger, Felix (2023): Security vs. civil liberties: How citizens cope with threat, restriction, and ideology. *Frontiers in Political Science*, 4. 1006711. <https://doi.org/10.3389/fpos.2022.1006711>
- Klauser, Joanna; Albert, Bruno; Lindenmeier, Christian; Hammer, Andreas; Freiling, Felix; Heckmann, Dirk und Pfeiffer, Sabine (2026): Telekommunikationsüberwachung am Scheideweg: Zur Regulierbarkeit des Zugriffs auf verschlüsselte Kommunikation. *Zeitschrift für Cyberstrafrecht – CyberStR* 1/2026, S. 17–23.
- Kostka, Genia; Steinacker, Léa und Meckel, Miriam (2023): Under big brother's watchful eye: Cross-country attitudes toward facial recognition technology. *Government Information Quarterly*, 40(1), 101761. <https://doi.org/10.1016/j.giq.2022.101761>
- Kühne, Sylvia (2019): Sanfte Überwachung? Eine Untersuchung zur Akzeptanz von digitalen Fingerabdrucktechnologien im Alltag. Dissertation, Universität Hamburg. URL: <https://ediss.sub.uni-hamburg.de/bitstream/ediss/8356/1/Dissertation.pdf> (besucht am 22.01.2026).
- Lawall, Alexander und Scharping, Davorin (2024): Staatstrojaner: Recht auf Privatsphäre: Analyse der Wirksamkeit der außerparlamentarischen Kontrollmechanismen. *Datenschutz und Datensicherheit - DuD*, 48(9), S. 603–607.
- Li, Robin G. (2024): Institutional trustworthiness on public attitudes toward facial recognition technology: Evidence from U.S. policing. *Government Information Quarterly*, 41(3), 101941. <https://doi.org/10.1016/j.giq.2024.101941>
- Lindenmeier, Christian; Gruber, Jan und Freiling, Felix (2024a): InveSTEE: A TEE-supported Framework for Lawful Remote Forensic Investigations. *Digital Threats: Research and Practice*, 5(3), S. 27:1–27:20. <https://doi.org/10.1145/3680294>

- Lindenmeier, Christian; Hammer, Andreas; Gruber, Jan; Röckl, Jonas und Freiling, Felix (2024b): Key extraction-based lawful access to encrypted data: Taxonomy and survey. *Forensic Science International: Digital Investigation*, 50, 301796. <https://doi.org/10.1016/j.fsidi.2024.301796>
- Lüdemann, Christian und Schlepper, Christina (2011): Der überwachte Bürger zwischen Apathie und Protest. Eine empirische Studie zum Widerstand gegen staatliche Kontrolle. In: Zurawski, Nils (Hrsg.): *Überwachungspraxen. Praktiken Der Überwachung Und Kontrolle*. Leverkusen: Budrich UniPress, S. 119–138.
- Lüdemann, Christian und Schlepper, Christina (2013): Angst im Überwachungsstaat: Eine empirische Studie zur Akzeptanz neuer staatlicher Kontrolltechnologien. In: Gaycken, Sandro (Hrsg.): *Jenseits von 1984 – Datenschutz und Überwachung in der fortgeschrittenen Informationsgesellschaft. Eine Versachlichung*. Bielefeld: transcript Verlag, S. 147–162. <https://doi.org/10.14361/transcript.9783839420034.147>
- Lyon, David (2007): *Surveillance Studies: An Overview*. Cambridge: Polity Press.
- Lyon, David und Haggerty, Kevin D. (2012): The surveillance legacies of 9/11: Recalling, reflecting on, and rethinking surveillance in the security era. *Canadian Journal of Law and Society/La Revue Canadienne Droit et Société*, 27(3), S. 291–300.
- Marcinkowski, Frank; Lünich, Marco; Anicker, Fabian; Flaßhoff, Florian G. und Keller, Birte (2026): Meinungsmonitor Künstliche Intelligenz 3.0. (Interaktives Dashboard). Düsseldorf: Heinrich-Heine-Universität. URL: <https://www.sozwiss.hhu.de/meinungsmmonitor-kuenstliche-intelligenz> (besucht am 25.01.2026)
- Marx, Gary T. (2015): Surveillance studies. *International Encyclopedia of the Social & Behavioral Sciences*, 23(2), S. 733–741.
- Moll, Ricarda und Schneider, Franziska (2021): Ausbau der Datenerhebungsbefugnisse von Sicherheitsbehörden – Lässt die wissenschaftliche Empirie Chilling-Effekte in der Bevölkerung erwarten? *Monatsschrift Für Kriminologie Und Strafrechtsreform*, 104(2), S. 92–106. <https://doi.org/10.1515/mks-2021-0113>
- Möller, Johanna; Schmitz, Lukas und Rehms, Sebastian (2025): Das Privacy Fabric Model: Ein Vorschlag für interdisziplinäre Verständigung in der Privatheitsforschung. In: Friedewald, Michael; Roßnagel, Alexander; Geminn, Christian L. und Karaboga, Murat (Hrsg.): *Freiheit in digitalen Infrastrukturen*. Baden-Baden: Nomos, S. 167–186.
- Mondak, Jeffery J. und Hurwitz, Jon (2012): Examining the Terror Exception: Terrorism and Commitments to Civil Liberties. *Public Opinion Quarterly*, 76(2), S. 193–213. <https://doi.org/10.1093/poq/nfr068>
- Patil, Sunil; Potoglou, Dimitris; Lu, Hui; Robinson, Neil und Burge, Peter (2014): Trade-off Across Privacy, Security and Surveillance in the Case of Metro Travel in Europe. *Transportation Research Procedia*, 1(1), S. 121–132. <https://doi.org/10.1016/j.trpro.2014.07.013>
- Pavone, Vincenzo und Degli Esposti, Sara (2012): Public assessment of new surveillance-oriented security technologies: Beyond the trade-off between privacy and security. *Public Understanding of Science*, 21(5), S. 556–572. <https://doi.org/10.1177/0963662510376886>
- Perkowski, Nina und Epik, Aziz (2024): Alltägliche (Un-) Sicherheit in Hamburg: Erkenntnisse Einer Partizipativen Studie. *Wissen Schafft Demokratie*, 16, S. 142–153.

- Petermann, Thomas und Scherz, Constanze (2005): TA und (Technik-) Akzeptanz (-forschung). *TATuP-Zeitschrift Für Technikfolgenabschätzung in Theorie Und Praxis*, 14(3), S. 45–53.
- Reddick, Christopher G.; Chatfield, Akemi T. und Jaramillo, Patricia A. (2015): Public opinion on National Security Agency surveillance programs: A multi-method approach. *Government Information Quarterly*, 32(2), S. 129–141. <https://doi.org/10.1016/j.giq.2015.01.003>
- Rehak, Rainer (2013): *Angezapft – Technische Möglichkeiten einer heimlichen Online-Durchsuchung und der Versuch ihrer rechtlichen Bändigung*. Münster: MV-Verlag Edition Wissenschaft.
- Trüdinger, Eva-Maria (2018): Sicherheit aus Vertrauen? Der Einfluss politischen und sozialen Vertrauens auf Präferenzen für staatliche Antiterrormaßnahmen. In: Steinbrecher, Markus; Biehl, Heiko; Bytzek, Evelyn und Rosar, Ulrich (Hrsg.): *Freiheit oder Sicherheit? Ein Spannungsverhältnis aus Sicht der Bürgerinnen und Bürger*. Wiesbaden: Springer Fachmedien, S. 77–100. https://doi.org/10.1007/978-3-658-23611-3_4
- Trüdinger, Eva-Maria und Steckermeier, Leonie C. (2017): Trusting and controlling? Political trust, information and acceptance of surveillance policies: The case of Germany. *Government Information Quarterly*, 34(3), S. 421–433. <https://doi.org/10.1016/j.giq.2017.07.003>
- Trüdinger, Eva-Maria und Ziller, Conrad (2022): Considered effective? How policy evaluations and threat perceptions affect support for surveillance in the context of terrorism. *Politics & Policy*, 50(5), S. 894–912. <https://doi.org/10.1111/polp.12498>
- Van den Broek, Tijs; Ooms, Merel; Friedewald, Michael; Van Lieshout, Marc und Rung, Sven (2017): Privacy and security: Citizens' desires for an equal footing. In: Friedewald, Michael; Burgess, Peter; Čas, Johann; Bellanova, Rocco und Walter, Peisl (Hrsg.): *Surveillance, privacy and security*. London: Routledge, S. 15–35.
- Van Heek, Julia; Arning, Katrin und Ziefle, Martina (2017): The Surveillance Society: Which Factors Form Public Acceptance of Surveillance Technologies? In: Helfert, Markus; Klein, Cornel; Donnellan, Brian und Gusikhin, Oleg (Hrsg.): *Smart Cities, Green Technologies, and Intelligent Transport Systems*. Cham: Springer International Publishing, S. 170–191. https://doi.org/10.1007/978-3-319-63712-9_10
- Vettermann, Oliver; Wagner, Manuela; Leicht, Maximilian und Freiling, Felix (2023): Lücken schließen: Der verantwortungsbewusste Umgang mit IT-Sicherheitslücken. München: bidt. <https://doi.org/10.35067/B0BJ-IM05>
- Wright, David; Gutwirth, Serge; Friedewald, Michael; De Hert, Paul; Langheinrich, Marc und Mosciro, Anna (2009): Privacy, trust and policy-making: Challenges and responses. *Computer Law & Security Review*, 25(1), S. 69–83.
- Zdun, Steffen (2006): Telekommunikationsüberwachung. In: Lange, Hans-Jürgen und Gasch, Matthias (Hrsg.): *Wörterbuch zur Inneren Sicherheit*. Wiesbaden: Springer, S.325-329. https://doi.org/10.1007/978-3-531-90596-9_79
- Ziller, Conrad und Helbling, Marc (2021): Public support for state surveillance. *European Journal of Political Research*, 60(4), S. 994–1006. <https://doi.org/10.1111/1475-6765.12424>

