Hochschule Bremen
City University of Applied Sciences

Prof. Dr. Dennis-Kenji Kipker · Flughafenallee 10 · 28199 Bremen

Deutscher Bundestag
Finanzausschuss
Der Vorsitzende

nachrichtlich per E-Mail

Bremen, 24.09.2023

Prof. Dr. Dennis-Kenji Kipker
Professor für IT-Sicherheitsrecht

Flughafenallee 10
28199 Bremen
T +49 421 5905 5465
dennis-kenji.kipker@hs-bremen.de

Prof. Dr. jur. Dennis-Kenji Kipker

Schriftliche Stellungnahme

Gesetzentwurf der Bundesregierung

Entwurf eines Gesetzes zur Stärkung der risikobasierten Arbeitsweise der Zentralstelle für Finanztransaktionsuntersuchungen

Drucksache 20/8294

Kernauftrag der Zentralstelle für Finanztransaktionsuntersuchungen (Financial Intelligence Unit/FIU) ist gem. § 27 Geldwäschegesetz (GwG) seit ihrer Gründung die Bekämpfung von Geldwäsche und Terrorismusfinanzierung, wobei ihr Handlungsauftrag bis zu den Terroranschlägen des 11. September 2001 in den USA zurückreicht. In der Analysetätigkeit der FIU und dem Informationsaustausch mit anderen Behörden kommt der „Filterfunktion" der Zentralstelle eine besondere Bedeutung zu. Die Aufgaben der Zentralstelle ergeben sich rechtlich insbesondere aus § 28 GwG. Bei der (verfassungs)rechtlichen Bewertung der Aufgaben der nationalen FIU ist zu berücksichtigen, dass es sich bei ihr nicht um eine Ermittlungs- oder Strafverfolgungsbehörde handelt. Vielmehr wird sie bereits unterhalb der Schwelle eines strafprozessualen Anfangsverdachts tätig. Ebenso einzustellen in die Bewertung ist, dass die FIU organisatorisch eigenständig arbeitet und im Rahmen ihrer Aufgaben und Befugnisse fachlich unabhängig handelt. Auch ist das Bundesministerium der Finanzen als Aufsichtsbehörde in bestimmten Fällen auf die Rechtsaufsicht beschränkt.

Zur Erfüllung des gesetzlichen Auftrages der FIU kommt der Erhebung und Analyse von Informationen und der Weitergabe von Informationen an die zuständigen inländischen öffentlichen Stellen eine erhebliche Bedeutung zu. Zur Erfüllung ihrer Aufgaben nimmt die FIU dabei nicht nur Meldungen nach dem GwG entgegen und sammelt diese, sondern führt auch operative Analysen und Bewertungen der Informationen durch. Die Zusammenarbeit mit externen Stellen erfasst im Hinblick auf die erlangten Informationen den Informationsaustausch und die Koordinierung mit inländischen Behörden, aber ebenso die Zusammenarbeit und den Informationsaustausch mit einschlägigen Einrichtungen anderer Staaten. Hierbei werden nicht nur die Informationen an sich übermittelt, sondern ebenso die Ergebnisse von operativen Analysen, entsprechende Typologien und Methoden. Außerdem in das Informationssystem einbezogen sind die für das Besteuerungsverfahren oder den Schutz der sozialen Sicherungssysteme zuständigen Behörden. Basierend auf den Erkenntnissen werden zusätzlich Jahresberichte veröffentlicht und Statistiken erstellt.

In den vergangenen Jahren wurde der Kreis der Meldeverpflichteten an die FIU ausgedehnt, auch wurden die Kriterien zur Abgabe von Verdachtsmeldungen nach GwG aktualisiert und die Zugriffsmöglichkeiten auf Datenbanken erweitert. Letztlich besteht immer dann eine Meldeverpflichtung an die FIU, wenn Anhaltspunkte darauf hindeuten, dass Vermögensgegenstände aus Straftaten stammen oder zur Terrorismusfinanzierung eingesetzt werden sollen. Um ihrer Zentralstellenfunktion nachzukommen, hat die FIU deshalb nicht nur Zugriff auf eigene Datenbanken, sondern auch die Möglichkeit des Zugriffs auf Datenbanken der öffentlichen Verwaltung. Dieser Zugriff erfasst unter anderem das Ausländerzentralregister (AZR), das Zentrale Staatsanwaltschaftliche Verfahrensregister (ZStV) und den Informationsverbund der Polizeibehörden (INPOL bzw. INPOL-neu), der beim Bundeskriminalamt (BKA) angesiedelt ist. Weitere Zugriffsmöglichkeiten der FIU betreffen steuerliche Grunddaten, Kontostammdaten und Veräußerungsanzeigen zum Grunderwerb. All diese Zugangsmöglichkeiten zu Datenbanken verschiedenster öffentlicher Einrichtungen zusätzlich zu den bestehenden Meldepflichten

an die FIU selbst verdeutlichen, dass nicht nur umfassende personenbezogene Datensätze verarbeitet werden, sondern auch sensible Daten von der Informationsverarbeitung der FIU betroffen sein können und sich umfassende Persönlichkeitsprofile bilden lassen.

Aus dem umfangreichen datenbezogenen Melde- und Zugriffswesen der FIU folgt, dass der Datenbestand der Einrichtung in erheblichen Maße wächst. Eine Gegenüberstellung der Auswertungen aus den Jahresberichten belegt dies deutlich: 2018 wurden 77.252 Meldungen angegeben, 2020 wurden 144.005 Meldungen angegeben, 2021 wurden 298.507 Meldungen angegeben. Ende Mai 2020 befanden sich 282.584 Verdachtsmeldungen im Informationspool der FIU (BT-Drs. 19/20953, S. 6). Gemessen an diesen erheblichen personenbezogenen Datensätzen wird die Informationsausbeute der FIU zunehmend als zu gering im Sinne der Erfüllung ihres gesetzlichen Auftrags kritisiert. So wird festgestellt, dass die FIU im Jahr 2020 lediglich 12.618 Rückmeldungen zu den weitergeleiteten Sachverhalten erhielt, von denen 79 zu einem Urteil führten. Daraus ergibt sich eine Quote von 0,6% (https://www.bfdi.bund.de/DE/Buerger/Inhalte/Polizei-Strafjustiz/National/FIU.html). Hinzu tritt, dass sich die FIU in Anbetracht der Vielzahl gemeldeter Daten außerstande sieht, sämtliche Verdachtsmeldungen zu bearbeiten. Im Oktober 2022 wurde in diesem Zusammenhang bekannt, dass mehr als 100.000 Verdachtsmeldungen unbearbeitet geblieben waren. Von den über 100.000 Verdachtsmeldungen wurden dabei nur 39.781 als relevant eingestuft. Hinzu tritt, dass die als nicht relevant eingestuften Meldungen im Infopool abgelegt werden, dessen Stand zu Ende September 2022 424.694 Datensätze betrug (https://www.zdf.de/nachrichten/politik/geldwaesche-fiu-verdachtsmeldung-wissler-100.html). In diesem Infopool werden die Daten in der Regel drei Jahre bis zur Löschung gespeichert.

Aus verfassungs- und datenschutzrechtlicher Perspektive ist eine derartige Kumulation von Informationen in vernetzten Datenbanken, ohne dass diese für die ursprünglich konkret bestimmten Zwecke zeitnah eingesetzt werden können, höchst problematisch. Die gegenwärtige Fassung des GwG wird dabei der datenschutzrechtlichen Relevanz des Aufgaben- und Befugniszuschnitts der FIU nicht gerecht, indem in § 29 Abs. 1 GwG lediglich festgestellt wird, dass die Einrichtung personenbezogene Daten verarbeiten darf, soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist. Hinzu treten die umfassenden weiteren Verarbeitungsbefugnisse für personenbezogene Daten, die nicht weiter konkretisiert werden. So darf die FIU gem. § 29 Abs. 2 GwG personenbezogene Daten, die sie zur Erfüllung ihrer Aufgaben gespeichert hat, mit anderen Daten abgleichen, wenn dies nach dem GwG oder nach einem anderen Gesetz zulässig ist. Gem. § 29 Abs. 3 GwG ist es der FIU gar gestattet, bei ihr vorhandene personenbezogene Daten zu Fortbildungszwecken oder zu statistischen Zwecken zu verarbeiten, sollte eine Datenanonymisierung zu diesen Zwecken nicht möglich sein. Flankiert werden die die Verarbeitung von personenbezogenen Daten betreffenden Vorschriften durch § 39 GwG, der die Anforderung für eine Errichtungsanordnung für jede automatisierte Datei mit personenbezogenen Daten enthält. Zwar ist das Bestehen einer solchen gesetzlichen Grundlage unter grundsätzlicher Einbeziehung auch des

Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) zu begrüßen, dennoch ist die gegenwärtig in § 39 Abs. 2 GwG bestimmte pauschale Maximalspeicherfrist von fünf Jahren ohne die Benennung weiterer Kriterien zu weit gefasst. Überdies wird die in § 39 Abs. 4 GwG beschriebene und ebenfalls abstrakte Anforderung, die Notwendigkeit der Weiterführung oder der Änderung der Errichtungsanordnung in „angemessenen Abständen" zu überprüfen, der verfassungsrechtlichen Dimension der umfassenden personenbezogenen Datennutzung durch die FIU im Sinne des rechtsstaatlichen Verhältnismäßigkeitsgrundsatzes nicht gerecht.

Mit dem vorliegenden Entwurf der Bundesregierung (Drs. 20/8294) vom 11.09.2023 für ein „Gesetz zur Stärkung der risikobasierten Arbeitsweise der Zentralstelle für Finanztransaktionsuntersuchungen" soll den geschilderten rechtlichen und praktischen Bedenken begegnet werden. Der Regierungsentwurf ist dabei vor dem Hintergrund insbesondere nachfolgender Fragestellungen und Probleme zu bewerten:

- **Frage 1:** Falls es zu einem Abgleich großer Datenmengen mit polizeilichen Datenbanken und Registern kommt, wie kann der Datenschutz im Sinne von Normenklarheit und Verhältnismäßigkeit gewährleistet werden?

- **Frage 2:** Wie können bei den Sicherheitsbehörden sinnvolle IT-Lösungen geschaffen werden, ohne grundrechtliche Werte des Rechtsstaats zu verletzen?

- **Frage 3:** Wie kann bei dem durch die FIU geplanten Einsatz von algorithmischen Methoden und maschinellem Lernen Diskriminierung in den Entscheidungen verhindert werden?

Zur Beantwortung der grundrechtlich geprägten Fragestellungen 1 und 2 ist vorab anzumerken, dass die verfassungsrechtlich geschützten Interessen der informationellen Freiheit (hier insbesondere des Rechts auf informationelle Selbstbestimmung als verfassungsrechtliche Ausprägung des Datenschutzes) in den Widerstreit zu den ebenfalls verfassungsrechtlich geschützten staatlichen Sicherheitsinteressen zu setzen sind (dazu vertiefend *Kipker*, Informationelle Freiheit und staatliche Sicherheit: Rechtliche Herausforderungen moderner Überwachungstechnologien). Dies führt dazu, dass es keine absoluten Interessenabwägungen zugunsten des einen oder anderen grundrechtlich geschützten Wertes geben kann. Die Maßstäbe, die an eine solche Regulierung der staatlichen Sicherheit gegenüber der informationellen Freiheit anzulegen sind, bestimmen sich anhand der mit einer Sicherheitsmaßnahme verbundenen Eingriffstiefe in die informationellen Grundrechte, nach der Komplexität der eingesetzten technischen Mittel und ihrer daraus resultierenden Fehleranfälligkeit sowie der Frage, ob eine Eingriffsmaßnahme für den Betroffenen in nicht erkennbarer Weise, d.h. verdeckt, stattfindet. Vor allem im Hinblick auf die mittlerweile technisch weit fortgeschrittenen Datenverarbeitungsvorgänge der Sicherheitsbehörden, die eine Vielzahl personenbezogener Daten automatisiert und ggf. KI-gestützt auswerten können, ist der informationelle Grundrechtsschutz aus präventiver Sicht zu verstärken und vor allem prozedural auszugestalten. Der Gesetzgeber

hat daher mehr als früher organisatorische und verfahrensrechtliche Vorkehrungen zu schaffen, die einer Verletzung der informationellen Sphäre des Betroffenen entgegenwirken. Insbesondere für die anhand der Eingriffstiefe von staatlichen Datenverarbeitungsmaßnahmen zu bestimmenden Rechtfertigungsmaßstäbe gilt: Je schwerwiegender eine Maßnahme und je hochrangiger ein betroffenes Recht ist, umso größer sind die an die Rechtfertigung zu stellenden Anforderungen.

Diese Erkenntnisse werden im Folgenden weiter vertieft und decken sich insoweit in konkretisierter Form mit den Erwägungen, die das BVerfG in seiner „Palantir-Entscheidung" zur automatisierten Datenanalyse (Urteil vom 16.02.2023, 1 BvR 1547/19 und 1 BvR 2634/20) getätigt hat.

Zur Frage 1:

Um informationelle Freiheit und Sicherheit im Rahmen der staatlichen Überwachungstätigkeit in einen Ausgleich zueinander zu bringen, sind folgende konkrete Vorgaben aufzustellen, die auch für die zu reformierenden Befugnisse der FIU nach GwG gelten müssen: Im Hinblick auf die festgestellte nicht geringe informationelle Eingriffstiefe der Datenerhebungsmaßnahmen und Datenauswertungen der FIU, die insbesondere aus dem erheblichen Umfang der Datenspeicherung, deren bislang gesetzlich nur rudimentär bestimmter Dauer und den zahlreichen Übermittlungsmöglichkeiten resultiert, lassen sich nachfolgende Vorgaben ableiten:

- Es sind besonders hohe Anforderungen an die Effektivität der angewandten Methoden sowie an die Anonymität von Datenverarbeitungsvorgängen zu stellen, die bislang nach geltendem Recht wie zuvor festgestellt nicht gewahrt sind. Auch der Regierungsentwurf des GwG nimmt hierauf nicht Bezug.

- Ein durch Datenverarbeitungsmaßnahmen der FIU Betroffener kann infolge der technischen Komplexität eingesetzter Mittel und der möglichen nachteiligen rechtlichen Folgen für ihn ebenfalls erwarten, dass grundlegende Anforderungen an die Datensicherheit gewahrt bleiben, die qua Gesetz zu definieren sind. Auch hier bleibt der Entwurf hinter den rechtlichen Erwartungen zurück.

- Darüber hinaus besteht für digital verarbeitete Datenbestände ein erhöhtes Manipulationsrisiko, sodass auch im Hinblick auf die Beweismitteltauglichkeit gewonnener Daten deren Authentizität und Integrität weitestmöglich zu garantieren sind. Dieser Vorgabe soll § 29 Abs 5 GwG-E Rechnung tragen, greift inhaltlich aber zu kurz, wenn er in seiner Zielsetzung losgelöst vom Stand der Technik lediglich auf die „rechtliche Verwendbarkeit" referenziert.

- Aufgrund der beliebigen Vervielfältigungsmöglichkeiten und der im GwG und weiteren Vorschriften vorgesehen umfassenden Übermittlungsbefugnisse digitaler Daten ist für den angemessenen Ausgleich zwischen informationeller Freiheit und staatlicher Sicherheit ferner zu gewährleisten, dass die

Zweckbindung einmal erlangter Datenbestände beachtet wird und, eng damit verbunden, bei der Einrichtung und Nutzung behördlicher Verbunddateien die Besonderheiten des informationellen Trennungsprinzips Berücksichtigung finden. Auch dieser Anforderung wird bislang im geltenden GwG nicht ausreichend Rechnung getragen. Der Regierungsentwurf adressiert diese Vorgabe u.a. in § 29 Abs. 2a GwG-E.

- Unter dem Gesichtspunkt eines staatlichen Eingriffs in die informationellen Grundrechte primär im Nachrichtendienst- und Gefahrenabwehrbereich sind die rechtlichen Kontroll- und Begrenzungsmöglichkeiten für angeordnete und getroffene Maßnahmen deutlich zu verbessern. Hierunter fallen vornehmlich behördliche Informationspflichten, Betroffenenrechte und Rechtsschutzmöglichkeiten. Hierauf wird bislang gesetzlich nicht Bezug genommen.

- Die Datenverarbeitungssysteme der FIU sind so auszugestalten, dass sie nur so wenige personenbezogene Daten wie möglich erheben, verarbeiten oder nutzen. Soweit möglich, ist bei der Datenverarbeitung eine Anonymisierung oder Pseudonymisierung durchzuführen. Dieser Grundsatz der Datenvermeidung und Datensparsamkeit sowie die informationelle Selbstbestimmung werden durch eine automatisierte Datenverarbeitung, innerhalb derer den Sicherheitsbehörden nur die tatsächlich für ein Ermittlungsverfahren relevanten Informationen zur Verfügung gestellt werden und sich der Personenbezug der verarbeiteten Daten im Regelfall der sicherheitsbehördlichen Kenntnisnahme entzieht, unter Berücksichtigung des Verarbeitungsziels verwirklicht. Diese Anforderung betrifft insbesondere solche Fälle, in denen eine Vielzahl personenbezogener Daten gleichzeitig verarbeitet wird. Weder das geltende GwG noch der Regierungsentwurf nehmen auf diese Vorgabe hinreichend Bezug.

- Der Gesetzgeber muss die wesentlichen Grundlagen zur Begrenzung von Art und Umfang der Daten und der Verarbeitungsmethoden selbst durch Gesetz vorgeben. Auch dies ist bislang im geltenden GwG nicht erfolgt. § 30 GwG-E wird diesen Vorgaben in der aktuellen Fassung ebenfalls nicht gerecht, da der Gesetzentwurf durch die Formulierung „Art und Umfang der Analyse haben sich am Risiko der Geldwäsche oder Terrorismusfinanzierung zu orientieren“ eine nach wie vor unbestimmte Zielvorgabe enthält. Inwieweit darüber hinaus der im Wesentlichen gleich gebliebene Pflichtenkatalog bei Aufstellung der Errichtungsanordnung nach § 39 GwG-E zu einer weiteren Konkretisierung über das geltende Recht hinaus beitragen soll, ist fraglich. Positiv hervorzuheben aber ist die angestrebte Änderung durch § 59 GwG-E, indem als milderes Mittel für den Informationsaustausch anstelle einer Datenübermittlung der zeitlich begrenzte Abruf bestimmt wird. Eine derartige Festsetzung sollte jedoch dauerhaft gesetzlich verankert werden.

- Abschließend sind konkrete und zeitnahe sowie an den datenschutzrechtlichen Zweckbindungsgrundsatz angelehnte Löschfristen zu definieren, was bislang ebenso nicht der Fall ist. Der Widerstreit zwischen Prognosesicherheit einerseits, die eine Vielzahl erhobener und ausgewerteter Datenbestände notwendig macht, und andererseits der Schutz des Betroffenen vor der Verarbeitung von Datenbeständen, die sich im Nachhinein als nicht notwendig zur Herbeiführung des Ermittlungserfolgs erweisen, kann nur dann in einen verhältnismäßigeren Ausgleich gebracht werden, wenn nicht jede beliebige Ermittlungsperson von jedem nur denkbaren Datum Kenntnis erlangt und solche Daten, die für Ermittlungen nicht zwingend benötigt werden, nach ihrer Aussonderung einer unverzüglichen Löschung unterfallen.

Zur Frage 2:

Sinnvolle sicherheitsbehördliche IT-Lösungen, die auch mit den rechtsstaatlichen Werten im Einklang stehen, setzen im Sinne eines „Grundrechtsschutzes durch Verfahren“ voraus, dass ein „Grundrechtsschutz durch Technikgestaltung“ realisiert wird. Ein solcher Grundrechtsschutz ist bislang für die Arbeit der FIU nicht erkennbar und sollte aufgrund der Eingriffsintensität der Auswertung einer Vielzahl personenbezogener Daten unter Überbrückung ursprünglicher Zweckbindungen dringend umgesetzt werden. Eine solche Forderung enthält auch die Palantir-Entscheidung des BVerfG, indem das Gericht klar bestimmt, dass soweit die Verwaltung zur näheren Regelung organisatorischer und technischer Einzelheiten bei der Durchführung automatisierter Datenanalyseverfahren ermächtigt wird, der Gesetzgeber immer noch zu gewährleisten hat, dass die Verwaltung die für die Durchführung einer automatisierten Datenanalyse oder -auswertung im Einzelfall maßgeblichen Vorgaben und Kriterien in abstrakt-genereller Form festlegt, verlässlich dokumentiert und in einer vom Gesetzgeber näher zu bestimmenden Weise veröffentlicht. Das sichert auch die verfassungsrechtlich gebotene Kontrolle, die insbesondere durch Datenschutzbeauftragte erfolgen kann.

Unter Berücksichtigung vorgenannter juristischer Erwägungen können deshalb nachfolgende technisch-organisatorische Maßnahmen bei der Datenverarbeitung der FIU vorausgesetzt werden bzw. unterstützend beitragen, um den verfassungs- und rechtsstaatlichen Grundsätzen zu genügen:

- Bereits bei der Bestimmung der dem Auswertungsverfahren zugrunde liegenden Datenquellen ist zu gewährleisten, dass keine unbegrenzte Zahl von Personen über einen manuellen Zugriff auf diese verfügt und es hierdurch zu einem intensiven Grundrechtseingriff infolge einer übermäßigen Verdichtung des behördlichen Informationsinteresses kommt. Es darf folglich nicht die Möglichkeit bestehen, dass vor dem Abgleich eine gesonderte Kenntnisnahme der Daten mit einer damit verbundenen Speicherung stattfindet, denn in einem derart konkretisierten Bereithalten der Daten zu Ermittlungszwecken ist bereits ein Grundrechtseingriff zu sehen. Nur durch einen solchen Zugriffsausschluss kann dem Erfordernis der unmittelbar im

Anschluss an die Datenerfassung stattfindenden Aussonderung Rechnung getragen werden. Falls es aus technischen Gründen nicht möglich sein sollte, die Datenerfassung vollständig gegenüber dem Zugriff durch Ermittlungs- bzw. Behördenpersonal abzuschirmen, sind die erhobenen Daten zumindest vor einer möglichen Kenntnisnahme sofort und automatisiert zu pseudonymisieren, wobei der Zuordnungsschlüssel technisch unzugänglich aufzubewahren ist, sodass trotz der theoretisch bestehenden Möglichkeit seitens der FIU zunächst kein Personenbezug hergestellt werden kann. Hierdurch kann die subjektive Grundrechtsbetroffenheit weitestgehend möglich ausgeschlossen werden.

- Um in der zweiten Phase der Datenverarbeitung, welche den eigentlichen Auswertungsvorgang betrifft, die Betroffenheit in den informationellen Grundrechten weiterhin so gering wie möglich zu halten, ist es notwendig, den unverzüglich auf die Datenerfassung folgenden Auswertungsvorgang autark zu gestalten, sodass das informationstechnische System selbstständig und unmittelbar die Überprüfung vornehmen kann, ob ein Datensatz für die Ermittlungen von weiterer Relevanz ist. Die Datenverarbeitung muss dazu in sich geschlossen ohne einen Zugriff durch Dritte datensicher stattfinden. Darüber hinaus ist die Vorgabe der Rasterkriterien hinreichend eng zu fassen, damit nicht auf diesem Wege eine zu große Anzahl von Trefferfällen generiert wird und auf diese Weise die grundrechtliche Eingriffsintensität der Auswertungsmaßnahme signifikant erhöht wird. Hierdurch wird sichergestellt, dass nur für tatsächliche Trefferfälle, welche nicht durch das vorgegebene Raster fallen, eine Zuordnung von Datenbeständen zu einer konkreten Einzelperson möglich ist, sodass die grundrechtliche Eingriffsintensität deutlich gegenüber dem aktuell bestehenden Verfahren der FIU reduziert wird.

- Abschließend sollten in einem dritten Schritt automatisch und sofort sämtliche Nichttrefferfälle gelöscht werden, wobei von dem Löschungsvorgang im Falle einer Pseudonymisierung der verarbeiteten Daten auch sämtliche Zuordnungsschlüssel umfasst sein müssen, sodass Rückschlüsse auf weitere Einzelpersonen über die Trefferfälle hinaus technisch unmöglich sind. Die ausgegebenen Trefferfälle sind nunmehr zwingend einer manuellen Überprüfung auf Richtigkeit und Plausibilität hin zu unterziehen, bevor weitere Entscheidungen und eventuelle Maßnahmen abgeleitet werden können.

Zur Frage 3:

Diskriminierung in sicherheitsbehördlichen Entscheidungen kann eine unberechtigte Kriminalisierung Betroffener zur Folge haben. Gerade für automatisierte und KI-gestützte Datenauswertungsverfahren ist das Potenzial von diskriminierenden Entscheidungen mittlerweile hinlänglich bekannt und bedarf an dieser Stelle deshalb keiner weiteren Ausführungen mehr.

Aus diesem Grunde ist es von Bedeutung, auf die Ermittlungsmethoden unserer Zeit zugeschnittene Maßnahmen zu entwickeln, welche vor einer unberechtigten Kriminalisierung schützen und damit letztlich einer Stigmatisierung von Personen vorbeugen, die für den Betroffenen nicht selten schwerwiegende soziale und wirtschaftliche Folgen nach sich zieht. Die Vermeidung von unberechtigten Kriminalisierungen gilt umso mehr, als dass Maßnahmen der öffentlichen Sicherheit in vielen Fällen als verdeckte Ermittlungsbefugnisse ausgestaltet sind, von welchen der Betroffene keine Kenntnis hat, sodass aufgrund der vorhandenen Möglichkeit zur Aussetzung der behördlichen Benachrichtigungspflicht gegenüber dem Betroffenen das Risiko besteht, dass dieser durch eine behördliche Ermittlungsmaßnahme zwar mittelbar benachteiligt wird, ihm jedoch die Benachteiligung als solche weder bekannt ist noch mangels seiner Kenntnis Rechtsschutzmaßnahmen dagegen ergriffen werden können.

Je mehr Daten erhoben und verarbeitet werden, umso größer ist auch die Gefahr, in ein bestimmtes, einer Datenauswertung zugrunde gelegtes Raster zu fallen und als sicherheitsbehördlich auffällig eingestuft zu werden, ohne dass ein polizeirechtlich relevantes oder kriminelles Verhalten objektiv erwiesen ist. Dies muss gerade für die FIU gelten. Um die informationelle Freiheit – hier insbesondere in den Ausprägungen des Rechts auf informationelle Selbstbestimmung und des Allgemeinen Persönlichkeitsrechts – und die staatliche Sicherheit zueinander in Ausgleich zu bringen, ist es folglich notwendig, zu verhindern, dass durch die technisch erweiterten Möglichkeiten der Filterung und Zusammenführung von Datenbeständen die Gefahr entsteht, dass durch Zufall jeder ein virtueller potenzieller Täter wird, lediglich weil er bestimmte Kriterien einer automatisierten Auswertung erfüllt. Nur derjenige, der den Rechtsfrieden tatsächlich bricht, muss im Zweifelsfall eine Sanktionierung durch die Öffentlichkeit erdulden, mit der sozial nachteilige Wirkungen für ihn verbunden sein können.

Folgende Maßnahmen werden deshalb zur Vorbeugung gegen Diskriminierung und damit verbunden einer unberechtigten Kriminalisierung durch automatisierte und KI-gestützte Datenauswertungsverfahren vorgeschlagen:

- **Festlegung hinreichend verlässlicher/sicherer Auswertungskriterien für automatisierte Datenauswertungen („Schwellenwerte“):** Die Qualität der Ergebnisse automatisierter Datenauswertungen zu Zwecken der öffentlichen Sicherheit ist in erster Linie von den zugrunde gelegten Auswertungskriterien abhängig, nach denen Personen in unterschiedliche Risikokategorien eingestuft werden. Auch die Behörden haben ein Interesse daran, dass solche Auswertungskriterien hinreichend sicher sind, indem sie keine unbeteiligten Personen kriminalisieren und auf diese Weise die Ermittlungsergebnisse verfälschen. Als Maßnahme zur Vermeidung solcher unberechtigten Kriminalisierung ist es notwendig, Erfordernisse auszumachen, die zu einer möglichst fehlerfreien automatisierten Datenauswertung beitragen können. Hierzu sollte verstärkt auf im Einzelfall bestehende Risikomuster zurückgegriffen werden bzw. diese sollten im Vorfeld ermittelt werden.

- **Transparenzherstellung und Öffentlichkeit der Entscheidungskriterien:** Der Vorwurf einer Diskriminierung kann zuvorderst durch Nachvollziehbarkeit der Entscheidungen ausgeräumt werden. Dies setzt Information vor allem der Öffentlichkeit voraus. Denkbar wäre unter rechtlichen Gesichtspunkten die Einbringung einer „Zwischenebene“ in der Form eines parlamentarischen Bürgervertreters für automatisierte behördliche Entscheidungsverfahren, vergleichbar dem „Beobachterstatus“ im Europäischen Parlament. Einem parlamentarischen Bürgervertreter käme im Bereich der staatlichen Schwellenwertbestimmung für automatisierte Auswertungsverfahren die Aufgabe der Transparenzherstellung zu, indem ihm investigative Befugnisse und ein Rederecht eingeräumt werden. Der Bürgervertreter kann beispielsweise von einem privaten Verein oder einer entsprechend datenschutzrechtlich befassten Organisation entsandt werden und braucht für seine Tätigkeit nicht demokratisch legitimiert zu sein. Turnusmäßig kann er ausgetauscht werden, sodass seine Neutralität gewahrt bleibt. Der parlamentarische Bürgervertreter kann der Bevölkerung als unmittelbarer Ansprechpartner zur Verfügung stehen, wenn es um Fragen der Kriminalisierung bestimmter Verhaltensweisen durch die Festlegung von Schwellenwertbestimmungen oder KI-gestützte Datenauswertungsverfahren geht und seine Bedenken in den parlamentarischen Diskurs einbringen, darüber hinaus aber auch im Generellen für die Herstellung von mehr Transparenz als Bestandteil des Rechtsstaatsprinzips im Bereich staatlicher Sicherheitsinteressen zuständig sein. Ihm sollte ferner die Kompetenz zuerkannt werden, innerhalb zu limitierender staatlicher Geheimhaltungsinteressen Anfragen aus der Bevölkerung zu beantworten, die sich mit dem Themenfeld der öffentlichen Sicherheit und automatisierter Datenauswertung befassen. Daneben muss er die Möglichkeit erhalten – ähnlich einem erweiterten Petitionsrecht – erhaltene Bürgereingaben unmittelbar in die Beratungen der jeweiligen Ausschüsse zu den Themen öffentlicher Sicherheit einzubringen. Indem der Öffentlichkeit auf diese Weise der Grundgedanke einer Einflussnahmemöglichkeit auf die Regulierung der staatlichen Überwachung nahegebracht wird, steigt die Akzeptanz gemeinschaftlich auferlegter Werte und das Misstrauen gegenüber einer unberechtigten Kriminalisierung durch automatisierte Datenverarbeitungsvorgänge wird reduziert. Auch unter Gesichtspunkten der Ausübung des Rechts auf informationelle Selbstbestimmung ist es entscheidend, dass alle potenziell Betroffenen einer sicherheitsbehördlichen Datenauswertung die Tragweite der Einschränkung ihres Selbstbestimmungsrechts richtig einschätzen können, wofür ihnen in einem gewissen Umfang auch Ziel und Grundrechtsbelastung von Maßnahmen offengelegt werden müssen. Wenn eine solche Offenlegung, wie insbesondere für den Fall des Rechts der öffentlichen Sicherheit, aufgrund staatlicher Geheimhaltungsinteressen grundsätzlich nicht unbegrenzt möglich sein sollte, ist zumindest die Beteiligung der

Öffentlichkeit am rechtspolitischen Diskurs sicherzustellen, wenn es um Eingriffsmaßnahmen geht, die jeden zu jeder Zeit unmittelbar betreffen können. Dies ist auch die FIU relevant, da auch im GwG staatliche Geheimhaltungsinteressen adressiert werden.

- **Nachgelagerte Überprüfungs- und Kontrollmaßnahmen, insb. für den Einsatz von Machine Learning:** Ein allgemeiner rechtlicher Grundsatz für den Einsatz von KI-gestützten Datenauswertungen ist aufgrund ihrer besonderen Risikoträchtigkeit der Verbleib der Letztentscheidung bei menschlichen Akteuren, insbesondere soweit das Ergebnis einer KI-gestützten Datenauswertung nachteilige Folgen für den Betroffenen haben kann. Insoweit wird auf die Beantwortung insbesondere der Frage 2 verwiesen, deren Beantwortung sich auf besondere verfahrensrechtliche Maßgaben bezieht. Eine ähnliche Vorgabe enthält bereits § 29 Abs. 2b GwG-E, indem bestimmt wird, dass bei einem Einsatz automatisierter Verfahren selbstlernende und automatisierte Systeme, die jeweils eigenständig Gefährlichkeitsaussagen über Personen treffen können, unzulässig sind.

Unter sämtlichen vorgenannten Gesichtspunkten bleibt der vorgelegte Regierungsentwurf des GwG im Zuge einer Gesamtbetrachtung inhaltlich weit hinter den skizzierten rechtlichen Anforderungen zurück, obwohl diese zumindest partiell erfüllt werden.

Bremen, den 23. September 2023

Prof. Dr. jur. Dennis-Kenji Kipker