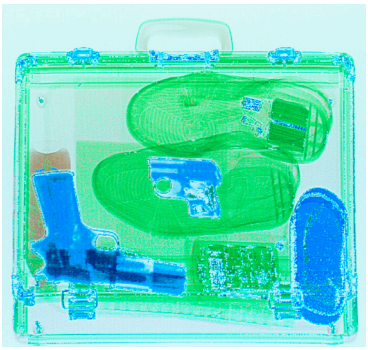
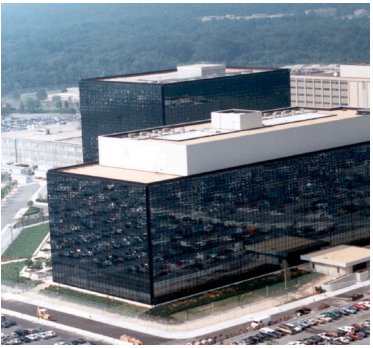
ArchiS
Architektur des Sicherheitsrechts

Marc Engelhart / Mehmet Arslan (Hrsg.)

Verbrechensbekämpfung durch Nachrichtendienste
Intelligence Services and Crime Control

BEITRÄGE ZUM SICHERHEITSRECHT


MAX-PLANCK-INSTITUT
ZUR ERFORSCHUNG VON
KRIMINALITÄT, SICHERHEIT UND RECHT

Marc Engelhart / Mehmet Arslan (Hrsg.)

Verbrechensbekämpfung durch Nachrichtendienste

Intelligence Services and Crime Control

Verbrechensbekämpfung durch Nachrichtendienste

Intelligence Services and Crime control

Marc Engelhart · Mehmet Arslan (Hrsg.)

Freiburg im Breisgau 2021

Contributions to Security Law/9
(Beiträge zum Sicherheitsrecht/9)

Edited by Marc Engelhart

The series entitled “Contributions to Security Law” is a venue that provides open access to important research findings for a broad spectrum of professionals. The findings are the results of projects, including ongoing projects, that emerged from the Otto-Hahn-Group on the “Architecture of Security Law” (ArchiS) or are projects of individual group members. The papers are available both online in PDF format on the websites of the Max Planck Institute for the Study of Crime, Security and Law (https://csl.mpg.de/) and the research group (https://criminallaw.science) as well as in print.

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Umschlagbild: © (v.l.n.r.) kyolshin, iStock; Flying Colours Ltd., Getty Images; tirc83, iStock [obere Reihe]; NSA, www.nsa.gov; mthaler, iStock [untere Reihe]

Satz: Ines Hofmann

Druck: Stückle Druck und Verlag, Stückle-Straße 1, 77955 Ettenheim

ISBN 978-3-86113-760-3

DOI https://doi.org/10.30709/archis-2020-9

Vorwort

Dieser Sammelband besteht aus Beiträgen des Workshops „Verbrechensbekämpfung durch Nachrichtendienste“, der vom 19. bis 20. Oktober 2018 am Max-Plank-Institut für ausländisches und internationales Strafrecht (jetzt Max-Planck-Institut zur Erforschung von Kriminalität, Sicherheit und Recht) in Freiburg i. Br. stattfand. Der Workshop zielte auf eine umfassende systematische Analyse der europäischen Nachrichtendienste im Hinblick auf deren zunehmende Bedeutung bei der Verbrechensbekämpfung.

Die Referentinnen und Referenten erhielten im Voraus einen Fragenkatalog, um den Themenkomplex anhand einer einheitlichen Struktur bearbeiten zu können, wobei es ihnen freigestellt war, eigene Schwerpunkte zu setzen, wenn sich dies in Bezug auf das jeweilige nationale Recht anbot. Detaillierte Ausführungen zum Fragenkatalog finden sich in der Einführung zum vorliegenden Band. Die Darstellung der wesentlichen Ergebnisse des Workshops (S. 294 ff.) orientiert sich ebenfalls an dessen Struktur. In den Vergleich sind auch Erkenntnisse aus Workshop-Beiträgen von Referentinnen und Referenten aus Frankreich, Deutschland, Österreich, Italien und Norwegen eingeflossen, die hier nicht abgedruckt werden konnten.

Anlässlich der Veröffentlichung dieses Bandes möchten wir uns bei Prof. Dr. Dr. h.c. mult. Ulrich Sieber als Direktor a.D. des Max-Planck-Instituts nicht nur für seinen Ansporn zum Forschen an den Schnittstellen des Strafrechts und des neuen Sicherheitsrechts, sondern auch für die großzügige Unterstützung bei der Organisation des Workshops bedanken.

Des Weiteren geht unser Dank an alle Teilnehmerinnen und Teilnehmer des Workshops für ihre wertvollen Beiträge.

Marc Engelhart — Freiburg, September 2021

Mehmet Arslan — Freiburg, September 2021

Preface

This book consists of reports written by the participants of a workshop entitled "Combating Crime through Intelligence Services," held from 19 to 20 October 2018 at the Max Planck Institute for Foreign and International Criminal Law (now the Max Planck Institute for the Study of Crime, Security and Law) in Freiburg. The workshop aimed to undertake a comprehensive study and systematic analysis of European intelligence services with regard to their increasing role in the fight against crime.

The speakers received a standardized catalog of questions in advance and were asked to use these questions as a framework to address the broad topic of the workshop, thus ensuring that the contributions had a common structure. Speakers were free, however, to determine their own areas of focus based on the specific features of the national legal order they analyzed. The catalog of questions is presented and discussed in the Introduction. Likewise, the comparative analysis (p. 307 ff.) at the end of the volume, which synthesizes the key findings from the workshop and the individual contributions, largely follows the structure of the question catalog. The comparative analysis also incorporates insights from workshop contributions by speakers from France, Germany, Austria, Italy, and Norway, which could not be printed here.

On the occasion of the publication of this book, we would like to thank Prof. Dr. Dr. h.c. mult. Ulrich Sieber, former Director of the Institute, not only for his encouraging us to research the intersections of criminal law and the new landscape of security law but also for his generous support in organizing the workshop.

Finally, our thanks go to all the participants in the workshop for their valuable contributions.

Marc Engelhart
Freiburg, September 2021

Mehmet Arslan
Freiburg, September 2021

Inhaltsverzeichnis / Table of contents

Autoren- und Herausgeberverzeichnis
List of authors and editors

Dr. Mehmet Arslan, LL.M., Guest at the Otto Hahn Research Group for the Architecture of Security Law at the Max Planck Institute for the Study of Crime, Security and Law, Freiburg i. Br. (Germany) [formerly Max Planck Institute for Foreign and International Criminal Law]

Dr. Els de Busser, Assistant Professor at Leiden University, Faculty of Governance and Global Affairs, Institute of Security and Global Affairs, Leiden (The Netherlands)

PD Dr. Marc Engelhart, Adjunct Professor of Criminal Law at Goethe University Frankfurt am Main and former Head of the Otto Hahn Research Group for the Architecture of Security Law at the Max Planck Institute for the Study of Crime, Security and Law, Freiburg i. Br. (Germany) (2012–2021) [formerly Max Planck Institute for Foreign and International Criminal Law]

Dr. C.W. (Constant Willem) Hijzen, Assistant Professor at Leiden University, Institute of Security and Global Affairs and Institute for History, Leiden (The Netherlands)

Dr. Erdem İzzet Külçür, Assistant Professor of Criminal Law at Ibni Haldun University, Faculty of Law, Istanbul (Turkey)

Dr. Kamen Lyubomirov Novikov, Lawyer in Sofia and Lecturer at Sofia University St. Kliment Ohridski, Sofia (Bulgaria)

Dr. Ágota Margit Szabóné, Public Prosecutor, Szeged (Hungary)

Maria Ntamadaki, LL.M. (Bonn), PhD candidate at the Institute of Criminal Law, Rheinische Friedrich-Wilhelms University of Bonn and Attorney at Law (admitted to the Athens Bar)

Dr. Johanna Rinceanu, LL.M., Senior Researcher in the Department of Criminal Law at the Max Planck Institute for the Study of Crime, Security and Law, Freiburg i. Br. (Germany)

Dr. Susana Sánchez Ferro, Professor of Constitutional Law at Universidad Autónoma de Madrid and Member of the Madrid Institute for Advanced Study, Madrid (Spain)

Dr. Nadine Zurkinden, Assistant Professor of Criminal Law at the University of Zurich, Faculty of Law, Zurich (Switzerland)

Einführung

Marc Engelhart und Mehmet Arslan

In einigen Bereichen der schweren Kriminalität, wie Terrorismus, Cybercrime, organisiertes Verbrechen oder Wirtschaftskriminalität, werden in zahlreichen Staaten zunehmend nationale Nachrichtendienste tätig, weil diese kriminellen Phänomene auch als Gefahr für die nationale Sicherheit betrachtet werden.[1] Gleichzeitig werden die nachrichtendienstlichen Ermittlungsbefugnisse ausgebaut. Hinzu kommt, dass Nachrichtendienste inzwischen über massenweise erhobene, auch strafrechtlich relevante Informationen verfügen. Infolgedessen nehmen sie bei der Verbrechenskontrolle und -bekämpfung eine neue Rolle ein.[2] Diese Entwicklung wirft die Frage nach den Grenzen der sicherheitsbehördlichen Tätigkeiten auf.

Um ein möglichst umfassendes Bild der Lage in den nationalen Rechtsordnungen herauszuarbeiten und dieses einer normativen Würdigung zu unterziehen, bedarf der Themenkomplex der Verbrechensbekämpfung durch Nachrichtendienste einer gründlichen Analyse unter drei Hauptgesichtspunkten: Erstens stellt sich die Frage

---

[1] *Vogel*, ZIS 2017, 28; *Engelhart*/*Arslan*, Security Architecture, S. 69.
[2] *Sieber*, Der Paradigmenwechsel, S. 360 ff.

nach der Aufteilung sicherheitsbehördlicher Aufgabenfelder, die uns einen ersten Eindruck von der nationalen Sicherheitsarchitektur vermitteln. Zweitens lassen sich hinsichtlich der Nachrichtendienste organisatorische, aufgabenbereichs- sowie befugnisbezogene Anhaltspunkte feststellen, die sie in eine gewisse Nähe zur Verbrechensbekämpfung rücken. Drittens sind die formellen Interaktionswege zwischen Nachrichtendiensten und Strafverfolgung und deren normative Regelung im positiven Recht von großer Bedeutung, um zu sehen, wie weit die Nachrichtendienste auch auf konkrete Fälle der Verbrechensbekämpfung einwirken. Die drei genannten Gesichtspunkte werden im Folgen detaillierter erörtert.

I. Sicherheitsbehördliche Aufgabenfelder – Grundzüge der nationalen Sicherheitsarchitektur

Sicherheitsbehördliche Aufgabenfelder lassen sich funktional in mehrere einzelne Bereiche aufteilen. Sicherheit im weitesten Sinne wird meist unter den Gesichtspunkten der Prävention und Repression gedacht. Diese Dichotomie wird verfeinert, wenn man die Prävention in nachrichtendienstliche Tätigkeiten und Gefahrenabwehr im Einzelfall unterteilt und die Repression durch die Exekutive auf die polizeiliche und staatsanwaltliche Strafverfolgung beschränkt.[3] Um diese Funktionenfelder voneinander deutlich zu unterscheiden, müssen sie einer Konzeption zugefügt werden, die wesentliche Unterscheidungsmerkmale benennt und diese definiert.

Erstens kann zwischen Zwecken der sicherheitsbehördlichen Aufgabenfelder unterschieden werden. Während etwa nachrichtendienstliche Tätigkeit sich dem engeren Bereich des Schutzes nationaler Sicherheit unter dem Aspekt der Souveränität widmet, so kann der Strafverfolgung etwa die Aufgabe zukommen, den Rechtsgüterschutz durch das Strafrecht zu fördern. Zweitens kann die lege artis Art und Weise des Tätigwerdens in einem Aufgabenfeld ein Unterscheidungsmerkmal darstellen, das den besonderen modus operandi der jeweiligen Funktion beschreibt. Bei nachrichtendienstlichen Tätigkeiten lassen sich die Generierung von Erkenntnissen durch Informationssammlung als Kernfunktion ausmachen, während sich etwa die polizeiliche Prävention der Beseitigung von störenden Ereignissen und der Abwehr von Gefahren im Einzelfall verschreibt. Drittens lassen sich sicherheitsbehördliche Aufgabenfelder unter dem Aspekt des Eingriffes und der Ermittlungsschwellen voneinander unterscheiden, an denen das jeweilige Tätigwerden ansetzt. Diese Schwellen können vom Vorliegen des Verdachts einer bestimmten Straftat, der Gefahr einer konkreten Störung bis hin zu einer abstrakten Gefahr im weitesten Sinne rangieren. Viertens kann eine gewisse Unterscheidbarkeit der jeweiligen Funktionsfelder durch die Mittel erreicht werden, mit denen diese Felder operieren. Anlasslose, einzelfall-

---

[3] Dieser Aufteilung kritisch gegenüber stehen *Griesbaum*/*Wallenta*, NStZ 2013, 369.

unabhängige, langfristige, flächendeckende und geheime Informationssammlungsmethoden eignen sich für die Nachrichtendienste, während etwa die Strafverfolgung durch personen- und anlassbezogene und grundsätzlich offene Ermittlungsmaßnahmen demonstrativ zum Rechtsgüterschutz beitragen.[4]

Die oben aufgeführten Eckpunkte einer sicherheitsbehördlichen Funktionsaufteilung ist lediglich skizzenhaft und keineswegs abschließend. Mit einer dadurch eingangs nur knapp dargestellten Konzeption soll dennoch der Weg bereitet werden, grobe Grundzüge einer nationalen Sicherheitsarchitektur sichtbar zu machen. Ob und inwieweit diese sich in den positivrechtlichen Bestimmungen widerspiegeln lassen, ist in erster Stelle nicht von essentieller Bedeutung. Im Fokus steht zunächst die Strukturfrage.[5]

Die derart in allgemeinen Zügen abgesteckte Struktur eignet sich als eine erste Annäherung, um das Themenfeld der Verbrechensbekämpfung durch Nachrichtendienste abzustecken. Das Verständnis der Sicherheitsarchitektur muss hinsichtlich der beiden Komponenten aber noch unter Berücksichtigung weiterer Aspekte vertieft werden. Die Vertiefung orientiert sich dabei an der Frage, ob und wieweit sich eine sog. Vernachrichtendienstlichung der präventiven oder repressiven Polizei feststellen lässt.

II. Die Nachrichtendienste

Anknüpfungspunkte für eine Operationalisierung der Nachrichtendienste für die Verbrechensbekämpfung lassen sich aus organisatorischen Besonderheiten der Dienste, deren strafverfolgungsrelevanten Aufgabenfeldern und neulich zunehmend aus weitreichenden Informationssammlungsmethoden gewinnen.

A. Organisatorische Besonderheiten

Im Allgemeinen sind die Nachrichtendienste dergestalt organisiert, dass sie mit der Regierung und/oder der Exekutive eng assoziiert sind. Während sie im ersten Fall die allgemeine politische Handlungsfähigkeit des Staates unterstützen sollen,[6] sind sie im zweiten Fall an der Durchsetzung einzelner exekutiver Entscheidungen beteiligt. Ihre Organisation richtet sich zumeist nach den geografischen oder bereichsspezifischen Schwerpunkten aus. Auslands und Inlandsdienste, die sich

---

[4] Zu den Unterscheidungsmerkmale im deutschen Sicherheitsrecht siehe eingehend *Gusy*, ZRP 1987, 48 ff.; *Arslan*, Intelligence and Crime Control, S. 523 f.

[5] Hierzu siehe auch *Würtenberger*/*Tanneberger*, Sicherheitsarchitektur als interdisziplinäres Forschungsfeld, S. 97.

[6] So etwa ausdrücklich deutsches Bundesverfassungsgericht, BVerfG NJW 2000, 63; siehe auch *Paeffgen*, StV 1999, 669.

militärische und zivile Aufklärung zum Ziel erklärt haben oder auch sich in national security intelligence oder law enforcement intelligence einteilen, sind gängige Organisationsformen. Zunehmend kommen hierbei Einheiten hinzu, die sich ausdrücklich der Erschließung von bestimmten Kriminalitätsbereichen, etwa Terrorismus oder Finanzdelikten, verschreiben.[7]

Weitere Anknüpfungspunkte organisatorischer Natur, die zeigen, wie weit sich die Nachrichtendienste für die Verbrechensbekämpfung fruchtbar machen lassen, können an Einzelheiten ihrer Binnenstruktur festgemacht werden. In diesem Zusammenhang ist die Frage von großer Bedeutung, ob die die jeweiligen Nachrichtendienste selbstständige Verwaltungseinheiten oder als eine Direktion oder Abteilung in eine übergreifende Sicherheitsbehörde integriert sind, z.B. ob der Finanznachrichtendienst beim Finanzministerium angesiedelt ist oder der Inlandsgeheimdienst in die Polizei eingegliedert ist, die auch eine repressive Sparte hat und Tätigkeiten einer Strafverfolgungsbehörde ausübt.

Anknüpfungspunkte organisatorischer Natur beschränken sich nicht auf die formelle klassische Verwaltungsorganisation. Auch informelle Gebilde wie Gremien, Zentren, Plattformen oder Datenbanken dienen zunehmend dazu, bei einer losen organisatorischen Bindung die Tätigkeit der nationalen Nachrichtendienste und Strafverfolgungsbehörden zu koordinieren oder den Informationsaustausch zwischen ihnen zu fördern.[8]

B. Strafverfolgungsrelevante Aufgabenfelder der Nachrichtendienste

Kriminalitätsfelder, in denen die Nachrichtendienste zum Schutz der nationalen Sicherheit etc. Beobachtungen anstellen und aufklärend tätig sind, sind nicht neu. Es sind klassische Verbrechensfelder, wie Spionage, Geheimnisverrat und Staatsschutzdelikte, die offenkundig für die nationale Sicherheit von Relevanz sind. Versteht man jedoch die nationale Sicherheit noch weiter als den klassischen Staatschutz und will man auch die Nachrichtendienste hierzu dienstbar machen, so fallen neuerdings weitere Kriminalitätsfelder, etwa transnationale Kriminalität, Cybercrime, Terrorismus, organisierte Kriminalität oder auch Wirtschafts-und Finanzdelikte bis zu einfachen Steuer- und Zolldelikten unter ein weit zu verstehendes Sicherheitskonzept.[9]

Eine solche Ausweitung der durch die Dienste nun zu überwachenden Kriminalitätsfelder und die dadurch entstandene Überlappung zwischen den Tätigkeitsfeldern der Nachrichtendienste und der Strafverfolgung können sowohl gesetzgeberisch

---

[7] Siehe etwa *Hütwohl*, ZIS 2017, 680 –687.

[8] *Sieber*, Der Paradigmenwechsel, S. 360 ff.

[9] Vgl. *Ibid*.

angestoßen worden sein oder sich auch in der Praxis bei bestehender Gesetzeslage eingebürgert haben.

C. Neue Befugnisse für eine effektive nachrichtendienstliche Verbrechensbekämpfung

Eine weitere Stelle, an der sich die Operationalisierung der Dienste für die Verbrechensbekämpfung gut beobachten lässt, betrifft die Gesetzgebungsaktivitäten, durch die die nationalen Nachrichtendienste in letzter Zeit neue Befugnisse für langfristige und flächendecke Überwachungsmaßnahmen erhalten haben.[10] Nicht selten spielt dabei das Argument, dass einige Bereiche der Kriminalität die nationale Sicherheit bedrohen und daher eine intensivere Aufklärung erforderlich machen, bei der Einführung neuer Überwachungsmaßnahmen der Nachrichtendienste eine Rolle. Entsprechenden Gesetzesvorhaben gehen ebenfalls nicht selten aufsehenerregende und medienwirksam aufgegriffene Attentate oder die Aufdeckung krimineller Strukturen voraus.

Der Ruf nach den Diensten zur Bekämpfung der Kriminalität hat seinen Preis. Die Dienste erhalten in letzter Zeit auch Befugnisse, mit denen sie über die Grenzen einer allgemeinen Informationssammlung hinaus drohende bzw. konkrete Gefahren, die von bestimmten Personen ausgehen (insbes. im Bereich der Terrorismusdelikte), aufdecken sollen.[11] Gleiches gilt, wenn etwa ein Finanznachrichtendienst etabliert wird, der sowohl potentiell gefährliche Transaktionen verhüten und verhindern als auch Fälle eines Straftatverdachts an die Strafverfolgung weitergeben soll.[12]

Die oben aufgeführten Berührungspunkte zwischen den Nachrichtendiensten und der Strafverfolgung sind nur beispielhaft und für eine Vertiefung des Themenkomplexes der Verbrechensbekämpfung durch Nachrichtendienste keineswegs abschließend.

III. Interaktion zwischen Nachrichtendiensten und Strafverfolgung

Die deskriptive Darstellung fördert bereits die ersten Interaktionsfelder zwischen Nachrichtendiensten und Strafverfolgung zutage, die darüber hinaus auch einer normativen Würdigung unterzogen werden müssen.

---

[10] Siehe etwa für Deutschland *Roggan*, Neue Aufgaben und Befugnisse im Geheimdienstrecht, S. 415 ff.

[11] Hierzu siehe eingehend *Chalkiadaki*, Gefährderkonzepte in der Kriminalpolitik, S. 109 ff.

[12] Vgl. *Hütwohl*, ZIS 2017, 681.

A. Im Allgemeinen

Normative Bewertungsmaßstäbe, die auf die Entwicklung im Nachrichtendienstrecht regulativ und korrektiv einwirken sollen, sind etwa in Deutschland nicht neu. So gewinnt beispielsweise das Trennungsgebot angesichts der neueren Entwicklungen zunehmend an Bedeutung. Es verlangt in seinen Grundzügen eine funktionale, organisatorische, personelle und informationelle Trennung zwischen Sicherheitsbehörden.[13] Zur Begründung dieses Gebots lassen sich einige zentrale Überlegungen anführen.

Erstens kann eine weitgehende Durchlässigkeit zwischen den Behörden den Grundrechtsschutz unterminieren, der entsprechend den Gedanken des Verhältnismäßigkeitsgrundsatzes nur unter bestimmten Voraussetzungen zum Schutz wichtiger Rechtsgüter und durch Eingriffe mit divergierender Intensität eingeschränkt werden darf. Eine funktionale Trennung ist insofern grundrechtsschutzimmanent.[14]

Zweitens ließe sich argumentieren, dass ohne eine Trennung die Entstehung eines „Supergeheimdienstes" drohe, der nicht nur beobachten, sondern Zwangsmaßnahmen anwenden und auch Strafklagen auf den Weg bringen kann. Es bestehe also die Gefahr, dass sich ein „Geheimdienst" entwickelt, der zu Zwecken der nationalen Sicherheit Zwang anwendet, sowie eine „Geheimpolizei", deren Gewalt Verdächtige ohne die Garantien des Strafprozessrechts ausgeliefert sind.[15]

Drittens scheint die Gewaltenteilung auch eine funktionale Trennung der Sicherheitsbehörden zu fordern.[16] Während die Nachrichtendienste die Handlungsfähigkeit der Regierung im Außen sowie deren nach innen gerichteten gesetzgeberischen Maßnahmen im Parlament unterstützen sollen, so soll der Exekutive ein Dienst zur Seite gestellt werden, der die Durchsetzung des Rechts in Gestalt der Abwehr störender Ereignisse betreibt. Schließlich ist die Judikative ebenfalls auf den Staatsanwalt und deren Hilfspersonen angewiesen, die die Anklagen vorbereiten und gerichtliche Entscheidungen umsetzen.

Ein ausdrücklich konzipiertes oder der Idee nach bestehendes Trennungsgebot ist eine Maximierungsvorgabe. Der Grad deren Umsetzung lässt sich insbesondere organisatorisch, personell und informationell vermessen.

---

[13] *Gusy*, ZRP 1987, 48 ff.; für seine verfassungsrechtliche Verankerung siehe BVerfG NJW 2013, 1505.

[14] Siehe etwa BVerfG NJW 2008, 831.

[15] Hierzu siehe etwa BVerfG NJW 2013, 1505.

[16] *Engelhart*/*Arslan*, Security Architecture, S. 11.

B. Organisatorische Trennung

Die Intensität der organisatorischen Trennung lässt sich unter mehreren Gesichtspunkten eruieren.

Erstens stellt sich dabei die Frage, ob die Nachrichtendienste bei der Beobachtung bestimmter Kriminalitätsfelder zusätzlich kriminalpolizeiliche Aufgaben haben oder sie entsprechende Befugnisse ausüben, wie etwa die Beweissicherung zum Zwecke einer späteren Anklageerhebung. Bejahendenfalls würde dies ein klarer Hinweis auf die Annäherung zwischen den Nachrichtendiensten und der Strafverfolgung darstellen. Somit würden funktional strafverfolgungsrelevante Aufgaben von einer nachrichtendienstlichen Organisation erledigt.

Zweitens ist die Konstellation in Betracht zu ziehen, ob bestimmte Sicherheitsbehörden, etwa die Polizei, sowohl eine nachrichtendienstliche als auch eine repressiv tätig werdende Einheit haben. In der Tat stellen polizeiliche Nachrichteneinheiten eine interessente Organisationsform dar. Sie rühren von der Idee einer ziemlich weit verstanden Prävention her, die nicht nur klassisch nachrichtendienstliche Informationssammlung umfassen soll, sondern auch die Gefahrenabwehr und die Strafverfolgung im Einzelfall. Daran lässt sich gut ersehen, wie eine Organisationsform eine funktionale Trennung unter Umständen aushebeln kann.

Drittens kann die organisatorische Trennung dadurch geschwächt werden, wenn bei der formell bestehenden Trennung die präventive Polizei im Vorfeld der konventionellen Ermittlungsschwelle zur Vorbereitung auf die Abwehr künftiger Gefahren Informationssammlung betreibt. Nichts anderes würde es bedeuten, wenn die Vorbereitung künftigen Strafverfahren dienen soll.[17] Auch hier schleicht sich die Idee einer ziemlich weit verstanden Prävention ein, die darum bemüht ist, die Gefahrenabwehr umfassend zu gewährleisten.

Viertens stellt sich die Frage, ob und inwiefern die polizeilichen Strafverfolgungsbehörden über die Grenzen der strafrechtlichen Aufklärung hinaus tätig werden.[18] Denn auch hier lässt sich eine Tendenz der Vorfelds- und Umfeldsicherung beobachten. Auch die Strafverfolgung ließe sich unter dem Dach einer weit verstanden Prävention in bestimmten Bereichen wie Staatsschutz, Terrorismus, oder Drogendelikte etc. als eine Art Output- oder auch Durchgangsstation konzipieren. Dies wird dann offenkundig zu Lasten eines klaren Trennungsgebots gehen.

---

[17] Hierzu siehe *Roggan*, NJW 2009, 262; *Daun*, Die deutschen Nachrichtendienste, S. 68.

[18] *Ibid*.

C. Personelle Trennung

Die Trennung zwischen den Nachrichtendiensten und der Strafverfolgung betrifft auch die personelle Organisation und Ausstattung der Behörden.

Erstens ist es dabei die Frage wichtig, ob die Beamte der Nachrichtendienste und die der Strafverfolgung zur selben Verwaltungseinheit gehören. Bejahendenfalls könnte etwa eine Ermittlungsperson auch nachrichtendienstlich tätig werden, oder auch umgekehrt. In einer Person würden sich dann unterschiedliche Dienstpflichten vereinigen.

Zweitens ist auch im Fall einer formellen personellen Trennung die Frage von Bedeutung, ob die Beamten der Nachrichtendienste auch vollzugspolizeiliche Befugnisse haben bzw. ob ihnen Erstzugriffsrechte zustehen oder sie für die Strafverfolgung Amtshilfe leisten und wie oft.[19]

Drittens stellt sich im Zusammenhang der personellen Trennung die Frage, ob zwischen den Nachrichtendiensten und Strafverfolgung ein personeller Austausch stattfindet und wie intensiv. Dabei ist auch der Umstand in Betracht zu ziehen, zu welchen Zwecken dieser Austausch auf den Weg gebracht wird. Eine Art intensive und umfassende Ausbildung der Strafverfolgungsbeamten für nachrichtendienstliche Tätigkeiten würde zu Lasten des Trennungsgebots gehen.

D. Informationelle Trennung

Schließlich muss das Vorhandensein der informationellen Trennung bzw. deren Reichweite eruiert werden. Die sich hierbei stellenden Fragen sind allen voran für das Strafverfahren von erheblicher Bedeutung. Um den Grad der informationellen Trennung zu bewerten, sind folgende Konstellationen in Betracht zu ziehen:

Erstens muss danach gefragt werden, ob die Rechtsordnung überhaupt den Informationsaustausch zwischen den nationalen Nachrichtendiensten und den Strafverfolgungsbehörden regelt. Etwaige Defizite können als Hinweis auf einen schwachen Grundrechtsschutz gesehen werden.[20] Dies kann unter Umständen dazu führen, dass ein durchgehend ungehinderter Informationsaustausch zwischen den nationalen Nachrichtendiensten und den Strafverfolgungsbehörden stattfindet. Dabei kann man von einer informationellen Einheit der beiden Tätigkeitsfelder sprechen kann.

---

[19] Hierzu siehe *Korte*, Informationsgewinnung der Nachrichtendienste, S. 45; *Nehm*, NJW 2004, 3289.

[20] Zur Entwicklung des deutschen Übermittlungsrechts im Wege des erweiterten Grundrechtsschutzes siehe *Engelhart*/*Arslan*, Security Architecture, S. 24; siehe auch *Gusy*, Polizei- und Ordnungsrecht, S. 37; *Paeffgen*, StV 1999, 676.

Zweitens ist bei gesetzlichen Regelungen hinsichtlich des Informationsaustausches weiter zu differenzieren. Je nach der Regelungsdichte lassen sich dabei beispielsweise Übermittlungspflichten für die nationalen Nachrichtendienste in bestimmten Fällen, von Amts wegen oder auf Anfrage/Anregung der Strafverfolgungsbehörden feststellen. Hinweise auf eine informationelle Trennung können Übermittlungsverbote für die nationalen Nachrichtendienste in bestimmten Fällen bzw. Anfrageverbote für die Strafverfolgungsbehörden darstellen. Allerdings ist dabei nicht außer Acht zu lassen, dass die Übermittlungsvorgänge aus unterschiedlichen Gründen den Nachrichtendiensten ungelegen sind. Dies kann dazu führen, dass die Übermittlung gesetzlich oder praktisch dem Ermessen der nationalen Nachrichtendienste überlassen ist und diese die Form und den Umfang der Übermittlung bestimmen.

In diesem Zusammenhang gewinnt die Frage an Bedeutung, durch welche Methoden die Dienste ihre Interessen im Strafverfahren schützen. So ist es möglich, dass sie zum Schutz ihrer Geheimnisse, die etwa ihre Arbeitsweise, Quellen oder Ermittlungsmethoden betreffen, den Strafverfolgungsbehörden nur eingeschränkt Informationen zukommen lassen.[21] Die Einschränkung kann im nationalen Recht etwa in Gestalt von Behördenzeugnissen bzw. Amtsberichten institutionalisiert sein oder auch völlig informell ohne irgendeinen Aktenvermerk erfolgen. Die Schutzmethoden sind nicht auf Ermittlungsverfahren eingeschränkt. Oft fordern die Dienste zum Schutz ihrer Geheimnisse bei der gerichtlichen Beweisaufnahme das Ergreifen besonderer Maßnahmen (Anonymisierung der Zeugen, Sperrung von Zeugen und Einführung von nachrichtendienstlichen Informationen durch Beweissurrogate, Zeugenvernehmung mithilfe Ton oder Bildübertragung, Schwärzung von Dokumenten, Bereitstellung von Zusammenfassungen, Fertigung von Behördengutachten oder Abhaltung eines In-camera-Verfahrens).[22] Die hierdurch tangierten Interessen der Verteidigung können durch verschiedenen Maßnahmen ausgeglichen werden, soweit die Methoden dies zulassen. Wichtige Instrumente sind im Hauptverfahren für das Gericht auch die Beweisverbotsregelungen. Ein schwacher Ausgleich für die Verteidigungsrechte im Strafverfahren würde nicht nur die informationelle Trennung unterminieren, sondern auch als Anzeichen dafür gedeutet werden können, dass auch das Strafverfahren Sicherheitsinteressen bzw. der Prävention im weitesten Sinne untergeordnet wird.

Schließlich lässt sich die informationelle Trennung im globalen Zeitalter ohne den Aspekt der internationalen Zusammenarbeit nicht beurteilen. Die oben aufgeführten Regelungsfragen stellen sich für das Phänomen der nachrichtendienstlichen Informationen ausländischer Dienste in einer besonderen Weise.[23] Denn dieser Weg der

---

[21] Hierzu siehe *Vogel*, ZIS 2017, S. 28.

[22] Hierzu eingehend *Frisch*, Der Schutz staatlicher Geheimnisse im Strafverfahren, S. 201.; siehe auch *Engelhart*/*Arslan*, Security Architecture, S. 95.

[23] Hierzu siehe *Schuster*, Verwertbarkeit im Ausland gewonnener Beweise im deutschen Strafprozess, passim.

Informationserlangung kann sich als ein geeignetes Konstrukt erweisen, sich beispielsweise nationalrechtlichen Grenzen eines Trennungsgebots zu entledigen.[24]

Literaturverzeichnis

Arslan, Mehmet, Intelligence and Crime Control in the Security Law of Germany in: The Limits of Criminal Law. Anglo-German Concepts and Principles, ed. by Matthew Dyson and Benjamin Vogel, 2018, Cambridge, 509–537.

Chalkiadaki, Vasiliki, Gefährderkonzepte in der Kriminalpolitik. Rechtsvergleichende Analyse der deutschen, französischen und englischen Ansätze. Wiesbaden 2015.

Daun, Anna, Die deutschen Nachrichtendienste, in: Thomas, Jäger/Anna, Daun (Hrsg.), Geheimdienste in Europa. Transformation, Kooperation und Kontrolle. Wiesbaden 2009, 56–77.

Engelhart, Marc/Arslan, Mehmet, Security Architecture in Germany. Freiburg 2020.

Frisch, Wolfgang, Der Schutz staatlicher Geheimnisse im Strafverfahren, in: Dünyada ve Türkiye'de Ceza Hukuku Reformları Kongresi, Sözüer Adem (Hrsg.), İstanbul 2013, Band 1, 201–230.

Griesbaum, Rainer/Wallenta, Frank, Strafverfolgung zur Verhinderung terroristischer Anschläge – Eine Bestandsaufnahme. NStZ 2013, 369–379.

Gusy, Christoph, Polizei- und Ordnungsrecht. 10. Auflage. Tübingen 2017.

Gusy, Christoph, Das verfassungsrechtliche Gebot der Trennung von Polizei und Nachrichtendiensten. ZRP 1987, 45–52.

Hütwohl, Mathias, Die Zentralstelle für Finanztransaktionsuntersuchungen (FIU) – Bekämpfung der Geldwäsche und Terrorismusfinanzierung nach dem neu gefassten Geldwäschegesetz. ZIS 11/2017, 680 –687.

Korte, Guido, Informationsgewinnung der Nachrichtendienste mit nachrichtendienstlichen Mitteln. Grenzen und Möglichkeiten der Informationsbeschaffung durch die Verfassungsschutzbehörden in: Guido, Korte/Manfred, Zoller (Hrsg.), Informationsgewinnung mit nachrichtendienstlichen Mitteln: Rahmenbedingungen, Einsatzmodalitäten, Verarbeitungsaspekte. Beiträge zur Inneren Sicherheit, Fachhochschule des Bundes. Oktober 2001. 35–88

Nehm, Kay, Das nachrichtendienstrechtliche Trennungsgebot und die neue Sicherheitsarchitektur. NJW 2004, 3289–3295.

Paeffgen, Hans-Ullrich, Das Urteil des Bundesverfassungsgerichts zum G 10 in der Fassung des Verbrechensbekämpfungsgesetzes 1994. StV 1999, 668–678.

Roggan, Fredrik, Das neue BKA-Gesetz – Zur weiteren Zentralisierung der deutschen Sicherheitsarchitektur. NJW 2009, 257–262.

---

[24] Vgl. Entscheidungen im Fall-Motassadeq OLG Hamburg, NJW 2005, 2326; BGH NJW 2007, 384.

Roggan, Fredrik, Neue Aufgaben und Befugnisse im Geheimdienstrecht in:Roggan/Kutscha (Hrsg.), Handbuch zum Recht der Inneren Sicherheit. 2. Auflage. Berlin 2006, S. 411–439.

Schuster, Frank Peter, Verwertbarkeit im Ausland gewonnener Beweise im deutschen Strafprozess. Berlin 2006.

Sieber, Ulrich, Der Paradigmenwechsel vom Strafrecht zum Sicherheitsrecht in: Tiedemann/Sieber/Burchard/Brodowski (Hrsg.), Die Verfassung moderner Strafrechtspflege. Erinnerung an Joachim Vogel, Baden-Baden 2016, 349–372.

Vogel, Benjamin, „In camera"-Verfahren als Gewährung effektiven Rechtsschutzes? Neue Entwicklungen im europäischen Sicherheitsrecht, ZIS 1/2017, 28–38.

Würtenberger, Thomas/Tanneberger, Steffen, Sicherheitsarchitektur als interdisziplinäres Forschungsfeld in: Riescher, Gisela (Hrsg.), Sicherheit und Freiheit statt Terror und Angst. Perspektiven einer demokratischen Sicherheit. 1. Auflage Freiburg 2010, 95–127.

Introduction

Marc Engelhart and Mehmet Arslan

In some areas of serious crime, such as terrorism, cybercrime, organized or economic crimes, the intelligence services are increasingly becoming involved in a number of states as these criminal phenomena are also viewed as a threat to national security.[1] At the same time, the intelligence services' powers of investigation are being widened. In addition, the services are collecting bulk data that is also relevant for criminal investigations.[2] As a result, they are assuming a new role in crime control and combating crime. This development again raises questions concerning the limits of security agency activities.

In order to work out a comprehensive picture of the situation regarding the national legal systems and to subject this to a normative assessment, the whole area of combating crime through the intelligence services requires a thorough analysis under three main headings. First, there is the question of the application of the remits of the security authorities, which gives us a first impression of the national security architecture. Second, organizational and other indicators, which relate to both remit and

---

[1] *Vogel*, ZIS 1/2017, 28; *Engelhart*/*Arslan*, Security Architecture, 69.

[2] *Sieber*, Der Paradigmenwechsel, 360 ff.

power, can be identified with regard to the intelligence services, bringing them closer to criminal prosecution. Third, the formal channels of interaction between the intelligence services and criminal prosecution, and their normative regulation in positive law, are of great importance in order to see how far the services have an impact on individual cases of combating crime. These three aspects are discussed in more detail below.

I. Remits of the security authorities – the basics of a national security architecture

The remits of the security authorities can be functionally divided into several task fields. Security, in the broadest sense, is usually thought of as prevention and repression. This dichotomy is refined if prevention is further divided into intelligence activities and averting danger in individual cases, and executive repression is limited to criminal prosecution by the police and the public prosecutor.[3] In order to clearly distinguish these remits functionally from one another, they must be embedded in a concept that names and defines some crucial distinguishing features.

First, a distinction can be made between the objectives of individual security remits. While intelligence, for instance, is devoted to protecting national security under the aspect of sovereignty, criminal prosecution can be given the task of the protection of legal goods through criminal law. Second, the *lege artis* way of operating in a security remit can be a distinguishing feature that describes the particular *modus operandi* of the respective function. In intelligence activities, the generation of knowledge through information gathering can be identified as the core function, while police prevention, for example, is focused on the removal of disturbance and averting danger in individual cases. Third, the remits of the security authorities can be distinguished from each another according to the type of investigation and intervention threshold at which the respective activity begins. These can range from the existence of a suspicion of a certain criminal offense and the danger of a specific disturbance, to an abstract risk in the broadest sense. Fourth, a certain distinguishability of the respective functional remits can be achieved through the means with which they operate. Secret and long-term information collection measures that are carried out without any factual specification, either temporally or personally (*anlasslos*), independent of any individual case and of a comprehensive nature, are suitable for the intelligence services, while criminal prosecution related to person and events, and basically open investigative measures, demonstratively contribute to the protection of legal goods.[4]

---

[3] Critical of this division, *Griesbaum*/*Wallenta*, NStZ 2013, 369.

[4] For the distinguishing traits in German security law, see *Gusy*, ZRP 1987, 48 f.; *Arslan*, Intelligence and Crime Control, 523.

The above-mentioned cornerstones of a functional division within the remits of the security authorities are roughly sketched and not conclusive. With a concept that is only briefly presented at the outset, the way should nevertheless be paved for making the basic features of a national security architecture visible. Whether and to what extent these can be reflected in positive legal provisions is primarily not of essential importance. The question of structure should initially be the focus.[5]

The general outline of such a structure would, however, be an approximation in order to cover the subject of combating crime by the intelligence services. An understanding of the security architecture in place must be deepened with regard to the two other components under review. This deepening should be based on the question of whether and to what extent a so-called "intelligencing", as described by German scholars (in the original, *Vernachrichtendienstlichung*), or securitization, of the preventive or repressive police can be determined.

II. Intelligence services

An idea of the connection factors involved in the operationalization of the intelligence services in the fight against crime can be gained from the organizational peculiarities of the services, their task fields with relevance to crime, and from recently increasingly expanded information collection measures.

A. Organizational peculiarities

In general, the intelligence services are organized in such a way that they are closely associated with the government and/or the executive branch. While in the first case they are intended to support the state's general political capacity to act in the broadest sense,[6] in the second they are involved in the implementation of individual executive decisions. They are organized with a geographical or thematical point of focus. The most common forms of organization are foreign and domestic services (civil or military), which generate national security intelligence or law enforcement intelligence. Increasingly, there are units that expressly commit themselves to exploit certain areas of crime, such as terrorism or financial crimes.[7]

Further connection factors of an organizational nature, to the extent to which the intelligence services can be utilized for combating crime, can be linked to details of

---

[5] See also *Würtenberger*/*Tanneberger*, Sicherheitsarchitektur als interdisziplinäres Forschungsfeld, 97 ff.

[6] Explicitly expressed by the German Federal Constitutional Court, BVerfG NJW 2000, 63; see also *Paeffgen*, StV 1999, 669.

[7] See also *Hütwohl*, ZIS 11/2017, 680–687.

their organization. In this context, the question of great importance is whether the respective intelligence services are independent administrative units or are integrated as a directorate or department in an overarching security authority, e.g., the financial intelligence service at the Ministry of Finance or the domestic intelligence service in the police force, which has a repressive branch and carries out measures of criminal prosecution.

Connection factors of an organizational nature are not limited to classical administrative organization forms. Informal entities, such as committees, centers, platforms or databases, under loose organizational links, are also increasingly being used to coordinate the activities of the national intelligence services and criminal prosecution authorities or to promote the exchange of information between them.[8]

B. Crime prosecution-related task fields of the intelligence services

Areas of crime on which the intelligence services collect information for the purpose of the protection of national security are not new. There are classic areas of crime, such as espionage, betrayal of state secrets and state security offenses, which are obviously relevant to national security. However, if one broadly understands national security going beyond the mere protection of the state and if one also wants to utilize the intelligence services in this regard, other fields of crime would fall under such a widely understood security concept, such as transnational crime, cybercrimes, terrorism, organized crime or even economic and financial offenses including tax and customs offenses.[9]

Such an expansion of the areas of crime currently being monitored by the services, and the resulting overlap between the remits of the intelligence services and criminal prosecution, has been initiated by the legislature or has evolved in legal practice.

C. New powers to effectively combat crime through the intelligence services

Another area where the operationalization of the intelligence services for combating crime can be clearly observed concerns legislation that has recently given these services new powers for long-term and comprehensive surveillance measures.[10] In this regard the argument is not uncommon that some areas of crime threaten national security and, therefore, require more intensive investigation when introducing new

---

[8] *Sieber*, Der Paradigmenwechsel, 360 ff.

[9] Ibid.

[10] See, for instance, for Germany, *Roggan*, Neue Aufgaben und Befugnisse im Geheimdienstrecht, 415 ff.

surveillance measures for the intelligence services. Corresponding legislative proposals are also often preceded by sensational attacks or the uncovering of criminal structures, which have been reported in the media extensively.

The call for services to combat crime comes at a price. The services have recently also been given powers that go beyond the collection of information in order to uncover imminent or specific dangers that arise from certain persons (especially in the case of terrorism offenses).[11] The same applies if, for example, a financial intelligence service is established to prevent and avert potentially dangerous/suspicious transactions, as well as to forward suspect cases to the criminal prosecution authorities.[12]

The connection factors mentioned above between the intelligence services and the criminal prosecution are only exemplary and not conclusive for a deepening understanding on the subject of combating crime by the intelligence services.

III. Interactions between the intelligence services and criminal prosecution

The above-presented descriptive account has already brought to light the first areas of interaction between the intelligence services and criminal prosecution, and this interaction must also be subjected to a normative assessment.

A. In general

Normative assessment criteria, which are intended to serve as regulative and corrective criteria in the field of intelligence law, are not new, for example, in Germany. In view of new developments with regard to the "intelligencing" or securitization of the criminal prosecution, the so-called principle of separation is becoming increasingly important. In its basic features it requires a functional, organizational, personal and informational separation between security authorities.[13] A few thoughts can be given to justify this principle.

First, extensive exchanges between the security authorities would undermine the protection of fundamental rights and, in particular, the principle of proportionality. According to this principle, these rights may only be restricted under certain conditions, which are different in each respective remit of security, and can lead to the

---

[11] For more detail see *Chalkiadaki*, Gefährderkonzepte in der Kriminalpolitik, 109 ff.

[12] See *Hütwohl*, ZIS 11/2017, S. 681.

[13] *Gusy*, ZRP 1987, 48 ff.; for constitutional anchoring of the principle of separation see BVerfG NJW 2013, 1505.

interference of fundamental rights with differing levels of intensity. Merging security branches with each other would abolish the balance that is set by the principle of proportionality. Thus, a functional separation seems to be inherent in the protection of fundamental rights.[14]

Second, it could be argued that if there is no separation, a "super-secret service" could emerge, which would not only observe and collect information but also use coercive measures and initiate criminal actions. The conclusion to this would be a "secret police" whose coercion against suspected persons would not be exposed without the guarantees of criminal procedure law.[15]

Third, the principle of separation of powers also seems to require a functional separation of the security authorities.[16] While the intelligence services are designed to support the government's ability to act abroad and enact legislative measures in parliament, the executive is to be provided with a service that enforces the law by removing and averting disturbance. After all, the judiciary is also dependent on the public prosecutor and their auxiliary persons who prepare the charges and implement judicial decisions.

An expressly or implicitly assumed principle of separation is to be maximized. The degree of their implementation can be measured with regard to organization, the peculiarities of the security services' personnel, and information exchanges between them.

B. Organizational separation

The intensity of the organizational separation, in particular, can be determined from several points of view.

First, the question arises as to whether the intelligence services have additional criminal investigation tasks when observing certain areas of crime or whether they exercise corresponding powers, for example, the securing of evidence for the purpose of future criminal actions. If so, this would be a clear indication of the rapprochement between the intelligence services and criminal prosecution. Thus, functionally criminal prosecution-related tasks would be carried out by an intelligence service.

Second, it should also be taken into account as to whether certain security authorities, such as the police, have both an intelligence and a criminal prosecution unit. In fact, police intelligence units represent an interesting form of organization. They stem from the idea of a broadly understood prevention method, which should not

---

[14] See, for instance, BVerfG NJW 2008, 831.

[15] In this regard, see BVerfG NJW 2013, 1505.

[16] *Engelhart*/*Arslan*, Security Architecture, 11.

only include the classic purpose of collection of intelligence information, but also an averting of specific dangers and criminal prosecution in individual cases. This clearly shows how a form of organization can undermine a functional separation under certain circumstances.

Third, the organizational separation can be weakened, even in the case of a formally acknowledged separation, if the preventive policy of collecting information happens in advance of the conventional investigation threshold for the purpose of the preparation of averting future dangers. The same would be true if said preparation were to serve future criminal proceedings.[17] Here, too, the idea of a broadly understood prevention method creeps in, which endeavors to ensure comprehensive protection against danger.

Fourth, the question arises as to whether and to what extent the police prosecution authorities act beyond the limits of criminal investigation.[18] Because, here, too, a tendency to secure the pre-field and the surrounding areas of a crime can be observed. Criminal prosecution could also be conceived as a kind of output or transit station under the umbrella of a broadly understood prevention method in certain areas, such as state security, terror, drug offenses, etc. This will obviously be at the expense of the principle of separation.

C. Personnel separation

The separation between the intelligence services and the criminal prosecution authorities also concerns the staffing (and its organization) of said authorities.

First, the pivotal question in this regard is whether intelligence officials and criminal prosecution officers belong to the same administrative unit. If so, an investigator would also have to act as an intelligence service officer, or vice versa. Different official duties would then be combined in one and the same person.

Second, even in the case of a formally acknowledged separation of personnel, the questions of whether the officers of the intelligence services also have law enforcement powers, i.e., to exercise coercion, or whether they provide administrative assistance for criminal prosecution and, if so, how often, are important.[19]

Third, in connection with the separation of personnel, the question arises whether there is an exchange of staff between the intelligence services and criminal prosecution and, if so, how intensely does this occur. The purpose for which this exchange

---

[17] For more on this see *Roggan*, NJW 2009, 262; *Daun*, Die deutschen Nachrichtendienste, 68.

[18] Ibid.

[19] For more on this see *Korte*, Informationsgewinnung der Nachrichtendienste, 45; *Nehm*, NJW 2004, 3289.

is brought about must also be taken into account. A kind of intensive and comprehensive training of criminal prosecution officers for intelligence activities would work at the expense of the principle of separation.

D. Informational separation

Finally, the existence of an informational separation or its range must be determined. The questions that arise here are of considerable importance for criminal proceedings. In order to evaluate the degree of informational separation, the following circumstances and possibilities should be considered:

First, the question should be asked whether the legal system regulates sharing of information between the national intelligence services and the criminal prosecution authorities. Respective shortcomings can be seen as an indication of a weak protection of fundamental rights.[20] Under certain circumstances, this can lead to an unhindered exchange of information between the national intelligence services and the criminal prosecution authorities. In this case, one can speak of an informational unit of the two remits.

Second, there is still a need to differentiate between the legal regulations regarding transmission of information between different security authorities. Depending on the density of regulations, transmission obligations for the national intelligence services can be determined in certain cases, *ex officio*, or at the request of the criminal prosecution authorities. Indications towards a separation of information would contain transmission prohibitions for the national intelligence services in certain cases or request prohibitions for the criminal prosecution authorities. However, it should not be forgotten that such transmissions may not be convenient for the intelligence services for various reasons. This can lead to a situation where the transmissions are legally or practically left to the discretion of the national intelligence services, which determine the form and scope of a certain transmission. In this context, the question of which methods the services use to protect their interests in criminal proceedings is becoming increasingly important. It is possible, for example, for them to only pass on restricted information to the criminal prosecution authorities in order to protect their secrets, such as those relating to their working methods, sources or investigation procedures.[21] The restriction can be institutionalized in national law, for example, by issuing certain types of official reports, or it can also be completely informal without any remark on the file. The protection methods are not limited to investigation proceedings. Often the services require special measures to be taken to protect their secrets during the court trial (anonymization of witnesses, blocking of witnesses and

---

[20] For the development of the protection of fundamental rights in this regard in Germany see *Engelhart*/*Arslan*, Security Architecture, 24; see also *Gusy*, Polizei- und Ordnungsrecht, 37; *Paeffgen*, StV 1999, 676.

[21] See also *Vogel*, ZIS 1/2017, 28 f.

introduction of intelligence information by means of hearsay evidence, hearing of witnesses using sound or image transmission, blackening of documents, providing of summaries, issuing of official reports or holding an in-camera session).[22] The interests of the defendant affected by these measures can be balanced by various countermeasures, as far as these used methods allow. Important instruments in the main proceedings for the court are also the exclusion rules on evidence. A weak compensation for the rights of defendants in criminal proceedings would not only undermine the informational separation but would also be regarded as an indication that such criminal proceedings were also subordinated to security interests or prevention, in the broadest sense.

Finally, the informational separation in the age of globalization cannot be assessed without international cooperation. The regulatory questions listed above arise in a special way for the phenomenon of intelligence information from foreign services.[23] This path of information gathering seems to be a suitable pretext to get rid of the national legal limits of the principle of separation.[24]

References

Arslan, Mehmet, Intelligence and Crime Control in the Security Law of Germany in: The Limits of Criminal Law. Anglo-German Concepts and Principles, ed. by Matthew Dyson and Benjamin Vogel, 2018, Cambridge, 509–537.

Chalkiadaki, Vasiliki, Gefährderkonzepte in der Kriminalpolitik. Rechtsvergleichende Analyse der deutschen, französischen und englischen Ansätze. Wiesbaden 2015.

Daun, Anna, Die deutschen Nachrichtendienste, in: Thomas, Jäger/Anna, Daun (eds), Geheimdienste in Europa. Transformation, Kooperation und Kontrolle. Wiesbaden 2009, 56–77.

Engelhart, Marc/Arslan, Mehmet, Security Architecture in Germany. Freiburg 2020.

Frisch, Wolfgang, Der Schutz staatlicher Geheimnisse im Strafverfahren, in: Dünyada ve Türkiye'de Ceza Hukuku Reformları Kongresi, Sözüer Adem (eds), İstanbul 2013, Volume 1, 201–230.

Griesbaum, Rainer/Wallenta, Frank, Strafverfolgung zur Verhinderung terroristischer Anschläge – Eine Bestandsaufnahme. NStZ 2013, 369–379.

Gusy, Christoph, Polizei- und Ordnungsrecht. 10. Auflage. Tübingen 2017.

---

[22] For more on this see *Frisch*, Der Schutz staatlicher Geheimnisse im Strafverfahren, 201 ff.; see also *Engelhart*/*Arslan*, Security Architecture, 95 ff.

[23] For more on this see *Schuster*, Frank Peter, Verwertbarkeit im Ausland gewonnener Beweise im deutschen Strafprozess. Berlin 2006. Passim.

[24] Compare with the decisions of German courts in the case of Motassadeq, OLG Hamburg, NJW 2005, 2326; BGH NJW 2007, 384.

Gusy, Christoph, Das verfassungsrechtliche Gebot der Trennung von Polizei und Nachrichtendiensten. ZRP 1987, 45–52.

Hütwohl, Mathias, Die Zentralstelle für Finanztransaktionsuntersuchungen (FIU) – Bekämpfung der Geldwäsche und Terrorismusfinanzierung nach dem neu gefassten Geldwäschegesetz. ZIS 11/2017, 680–687.

Korte, Guido, Informationsgewinnung der Nachrichtendienste mit nachrichtendienstlichen Mitteln. Grenzen und Möglichkeiten der Informationsbeschaffung durch die Verfassungsschutzbehörden in: Guido, Korte/Manfred, Zoller (eds), Informationsgewinnung mit nachrichtendienstlichen Mitteln: Rahmenbedingungen, Einsatzmodalitäten, Verarbeitungsaspekte. Beiträge zur Inneren Sicherheit, Fachhochschule des Bundes. Oktober 2001 35–88.

Nehm, Kay, Das nachrichtendienstrechtliche Trennungsgebot und die neue Sicherheitsarchitektur. NJW 2004, 3289–3295.

Paeffgen, Hans-Ullrich, Das Urteil des Bundesverfassungsgerichts zum G 10 in der Fassung des Verbrechensbekämpfungsgesetzes 1994. StV 1999, 668–678.

Roggan, Fredrik, Das neue BKA-Gesetz – Zur weiteren Zentralisierung der deutschen Sicherheitsarchitektur. NJW 2009, 257–262.

Roggan, Fredrik, Neue Aufgaben und Befugnisse im Geheimdienstrecht in:Roggan/Kutscha (eds), Handbuch zum Recht der Inneren Sicherheit. 2. Auflage. Berlin 2006, 411–439.

Schuster, Frank Peter, Verwertbarkeit im Ausland gewonnener Beweise im deutschen Strafprozess. Berlin 2006.

Sieber, Ulrich, Der Paradigmenwechsel vom Strafrecht zum Sicherheitsrecht in: Tiedemann/Sieber/Burchard/Brodowski (eds), Die Verfassung moderner Strafrechtspflege. Erinnerung an Joachim Vogel, Baden-Baden 2016, 349–372.

Vogel, Benjamin, „In camera"-Verfahren als Gewährung effektiven Rechtsschutzes? Neue Entwicklungen im europäischen Sicherheitsrecht, ZIS 1/2017, 28–38.

Würtenberger, Thomas/Tanneberger, Steffen, Sicherheitsarchitektur als interdisziplinäres Forschungsfeld in: Riescher, Gisela (eds), Sicherheit und Freiheit statt Terror und Angst. Perspektiven einer demokratischen Sicherheit. 1. Auflage Freiburg 2010, 95–127.

Belgian Intelligence Services and Crime Prosecution

Els de Busser

I. Background

The Belgian legal framework of intelligence and security services consists of one general law – the 1998 Law on the Intelligence and Security Services – that has since 2010 been the subject of three major amendments.[1] For this reason, the law will be referred to further in this report as the 1998 Consolidated Act.[2] It is important to

[1] See *Jacques* and *Van Caeneghem*, Monthly data collection on the current reform of intelligence legislation – Belgium, Milieu Ltd (2017).

[2] Act of 30 November 1998 on the Intelligence and Security Services, B.S. 18 December 1998 as amended by the Law of 30 March 2017, B.S. 28 April 2017 (further: 1998 Consolidated Act).

highlight that when it entered into force, the 1998 Law only provided for intelligence gathering via human sources and surveillance in public spaces.[3] The Belgian intelligence services were considered too restricted in their capabilities in comparison to Belgian police authorities and in comparison to their foreign counterparts. Three successive and substantial amendments to the 1998 Law were therefore considered necessary.

First, the specific methods of gathering data by intelligence and security services were laid down in a separate legal act of 2010, which made changes to the 1998 Consolidated Act.[4] The second significant amendment was triggered by a general reform of the Belgian justice system initiated in spring 2015 by Minister of Justice Koen Geens and aiming to increase the system's speed, efficiency and fairness.[5] A third substantial amending legal act was initiated shortly after the terrorist attacks in Paris and Brussels in, respectively, November 2015 and March 2016. This particular law expanded the intelligence services' competences with regard to surveillance.[6] The current report will narrow in on all relevant modifications to the 1998 Law.

In accordance with the 1998 Consolidated Act, the Belgian intelligence[7] and security services are organised in two agencies: the State Security Service (*Veiligheid van de Staat*) is competent for civil intelligence and security whereas the General Service for Intelligence and Security (*Algemene Dienst Inlichtingen en Veiligheid*) covers military intelligence and security.[8] For the purposes of this report, the State Security Service will be the focal point.

This country report will narrow in on the competences of the Belgian intelligence authorities; more specifically the organisational structures, the distinction in personnel and the distinction between information gathering methods will be studied. Finally, the cooperation between the Belgian intelligence and police authorities will be analysed.

---

[3] *Lasoen*, 32 International Journal of Intelligence and Counterintelligence 4 (2019).

[4] Act of 4 February 2010 on the methods for gathering data by intelligence and security services, B.S. 10 March 2010.

[5] Act of 5 February 2016 amending the acts on criminal justice and criminal procedure and containing diverse provisions on justice, B.S. 19 February 2016. For the full presentation of the so-called "Justice Plan", see https://cdn.nimbu.io/s/1jn2gqe/assets/Plan_justitie_18maart_NL.pdf

[6] Act of 30 March 2017 amending the act of 30 November 1998 on the Intelligence and Security Services and of Article 259 bis of the Criminal Code, B.S. 28 April 2017.

[7] For the purpose of this report, the term "intelligence authorities" will be used as a general term for referring to the intelligence and security authorities.

[8] Article 2 of the 1998 Consolidated Act.

II. Organisation

In accordance with Article 4 of the 1998 Consolidated Act, the Belgian intelligence authorities operate under the authority of the Minister of Justice and corresponding to the guidelines of the National Security Council. The Minister of Justice has the lead role in the organisation and the general administration of the State Security Service. Two stipulations are essential in this respect: the composition of the National Security Council and the power of the Minister of Home Affairs to order the State Security Service's cooperation.

First, the National Security Council is a body established by Royal Decree for the purpose of coordinating the general intelligence and security policy and determining the priorities in relation to intelligence and security.[9] The Council replaces the Ministerial Committee for Intelligence and Security that had been operational since 1996. Besides replacing the latter, the National Security Council has a broader composition in comparison to the Ministerial Committee. Presided by the Prime Minister and consisting of the Ministers of Justice, Defence, Home Affairs and Foreign Affairs, the Council also includes the head of the State Security Service, the head of the General Service for Intelligence and Security, the head of the federal police, the director of the threat analysis unit OCAD, the chair of the Directing Committee of the Federal Service of Home Affairs, a representative of the College of Prosecutors-General and the Federal Prosecutor. All other ministries can be present in the person of their Deputy Minister. Due to this wide composition and due to the leading role of the Prime Minister, who calls for the meetings of the Council and sets the agenda, the Council can influence the workings of the State Security Service. The Belgian federal police having a seat at the table in the National Security Council shows the connection with the tasks of the State Security Service.

Second, Article 5 §2 of the 1998 Consolidated Act specifies that the Minister of Home Affairs has the competence to claim the cooperation of the State Security Service in the carrying out of its core tasks when these are related to the maintaining of public order and the protection of persons. This special competence does not allow the Minister of Home Affairs to interfere with the organisation of the State Security Service but it does allow him to give recommendations and precise instructions as to the methods and the budget to be used. Taking into account that the Belgian federal police falls under the portfolio of both the Minister of Justice and the Minister of Home Affairs, this special competence demonstrates their organisational interrelatedness.

Besides the twofold organisational structure in State Security Service and General Service for Intelligence and Security, an academic study has shed a different light on the matter. Patrick Leroy – a member of the General Service for Intelligence and Security – argues that the Belgian intelligence community lacks a contextual

[9] Royal Decree of 28 January 2015 establishing the National Security Council, B.S. 30 January 2015.

definition.[10] Too much attention seems awarded to the organisational and hierarchical structures, whereas the intelligence community is not a closed network. Opening up the perspective on the intelligence community in an innovative manner, Leroy concludes that *de facto* it should be considered to also include specific departments of the federal police,[11] customs authorities, the Belgian Financial Intelligence Unit as well as the academic world represented by the Belgian Centre for Intelligence Studies and the training centre for intelligence and security services: the Belgian Intelligence Academy. Nevertheless, this broader and ground-breaking definition of the Belgian intelligence field goes beyond the scope of this report.

III. Personnel

The most recent activity report published by the Belgian State Security Service clarifies the slight increase in staff to reach 627 full-time equivalents in January 2018. Nominally, this means 30 additional full-time equivalents were hired since 2014. However, besides the retirement of several staff members, 46 protection officials were transferred to the federal police and the task of "close protection" was transferred to the police authorities following the abolishment of the department "Protection of Persons" at the State Security Service.[12] The actual number of new hires between 2016 and 2018 is 140, which does not yet amount to the doubling of staff members deemed necessary by its director as included in the report by the Parliamentary Commission investigating the Brussels terrorist attacks.[13] The increase in budget from 48,665 million Euros in 2017 to 63,441 million Euros in 2018 is largely explained by an investment in IT infrastructure rather than in personnel.[14]

In general, staff members of the State Security Service do not have police or judicial competences. An important exception to this principle is the protection of all staff of the intelligence authorities. A 2017 amendment to the 1998 Consolidated Act aimed to offer more protection to intelligence services' staff to carry out their tasks safely in a context of terrorist threats. For that purpose, an internal intervention team

---

[10] *Leroy*, 12 Revue militaire belge 91 (2016).

[11] Belgium has a complicated structure of federal and local police authorities which together form the integrated police (see Law 7 December 1998 on the establishment of an integrated police, organised on two levels, B.S. 5 January 1999). For the purpose of this report the federal police will be the focal point.

[12] Activity Report State Security Service 2017–2018, p. 8 and Act of 21 April 2016 on Interior Affairs and Integrated Police, B.S. 29 April 2016.

[13] Activity Report State Security Service 2017–2018, p. 8 and Chambre, 1752/008, Parliamentary Investigation into the circumstances that led to the terrorist attacks of 22 March 2016 in Zaventem airport and in metrostation Maalbeek, Brussels including the evolution and the handling of the fight against radicalism and terrorist threats, Third Interim Report on "Security Architecture", 15 June 2017, p. 273.

[14] Activity Report State Security Service 2017–2018, p. 8.

was set up rather than relying on the intervention by police authorities or on a right to self-defence. The choice for an internal team was made in order to react faster and more discreetly to on-going intelligence operations but also because information on on-going intelligence operations is classified and therefore not necessarily accessible to any police officers who would react to a call for assistance.[15] A new chapter III/1 on the protection of staff, infrastructure and goods of the intelligence and security authorities was therefore inserted in the 1998 Consolidated Act. The members of the internal intervention team are the only State Security Service officials who have limited police competences. Without such competences they would not be able to compel an individual behaving suspiciously on the authorities' premises or in the proximity thereof to identify him or herself.[16] They are not allowed to use these powers in the exercising of their other tasks as State Security Service officials.[17] The mentioned limited police powers include entering buildings, security check of persons, search of vehicles, confiscation, deprivation of liberty for the time necessary to transfer the person to police authorities, identity check, use of violence, use of firearms, and requiring assistance of third parties.[18]

When a State Security Service staff member in the ordinary carrying out of his or her duties encounters facts that may constitute criminal offences, the information should be transferred to the competent prosecution authority. This obligation rests on every Belgian civil servant by virtue of Article 29 of the Criminal Procedure Code.[19] The specific topic of information transfer will be covered more elaborately further in this report.

State Security Service officials can deliver technical assistance to judicial and administrative authorities provided that the assistance is requested by the recipient and respects the modalities and limitations laid down by both competent Ministers and the National Security Council.[20] Several recommendations included in the most recent activity report published by Standing Committee I show the need for the competent Ministers and the National Security Council to not only specify these modalities and limitations but also warn the security services not to use their intelligence gathering competences for the purposes of criminal prosecution.[21]

---

[15] Chambre, 2043/001, Legislative proposal for amending the Act of 30 November 1998 on the organisation of the intelligence and security service and of Article 259 bis of the Criminal Code, Travaux Préparatoires, 20 September 2016, p. 16.

[16] Ibid. p. 74.

[17] Article 22 of the 1998 Consolidated Act.

[18] Chambre, 2043/001, Legislative proposal for amending the Act of 30 November 1998 on the organisation of the intelligence and security service and of Article 259 bis of the Criminal Code, Travaux Préparatoires, 20 September 2016, p. 17.

[19] *Van Laethem*, 2 EJIS 6 (2008).

[20] Article 20, §2 of the 1998 Consolidated Act.

[21] Standing Committee I, Activity Report 2017, Intersentia, 2018, p. 130, 133 and 136.

IV. Competences

The principal competence of the Belgian State Security Service is to collect, analyse and process information related to every activity that threatens or could threaten the internal security of the state and the continuance of the democratic and constitutional order, the external security of the state and international relations, scientific or economic potential, or any other fundamental interest of the country. The activities that could fall within the scope of this definition are further specified in Article 7 of the 1998 Consolidated Act and include espionage, terrorism, extremism, proliferation and criminal organisations. The Federal police's department of judicial police has the competence to investigate and collect evidential material in relation to criminal acts, to find and arrest the offenders and to put them at the disposal of the competent authority in accordance with the applicable laws. Logically, this includes the acts mentioned in the competence of the State Security Service. Therefore, not only should the modalities of a transfer of information from the State Security Service to the Federal police be defined, but duplication of efforts should also be avoided and sharing of relevant information should be encouraged. Nevertheless, practice has shown that the latter is not always the case. This subsection will firstly narrow in on the legal provisions in the Belgian legal framework that organise the distinction between the State Security Service and the Federal police. Secondly, the transfer of information will be discussed.

A. General competence

The above-mentioned definition of the State Security Service's principal competence requires a closer study of its components. Moreover, it should be stressed that this is only the principal competence, besides the competence to conduct security assessments and the gathering, analysing and processing of information in relation to the activities of foreign intelligence authorities on Belgian territory.[22]

The role of the State Security Service is restricted to gathering information, analysing and processing it. This means that it does not have the power to counteract any threats that it may detect. Unlike some foreign counterparts, the Belgian intelligence services are defensive authorities whose mandate is aimed at defending the country from a range of threats but they lack the competence to act themselves.[23] Upon detection of a potential threat, the State Security Service should transfer the

---

[22] Article 7 of the 1998 Consolidated Act.

[23] Activity Report State Security Service 2017–2018, p. 8 and Chambre, 1752/008, Parliamentary Investigation into the circumstances that led to the terrorist attacks of 22 March 2016 in Zaventem airport and in metrostation Maalbeek, Brussels including the evolution and the handling of the fight against radicalism and terrorist threats, Third Interim Report on "Security Architecture", 15 June 2017, p. 267.

necessary information to the competent government authority.[24] In the case of a breach of provisions of the Criminal Code, the transfer should be done to the competent police authority. The Federal police's competences are not restricted in this manner. On the contrary, the power to take action upon discovery of a criminal act is what makes up a large part of the Federal police's tasks.

B. Specific material competence

The 1998 Consolidated Act includes its own definitions for all types of activities within the scope of the State Security Service. Remarkably, these definitions do not necessarily correspond to the description of the activities in accordance with the Belgian Criminal Code.[25] For example, terrorism is defined in the 1998 Consolidated Act as the use of violence against persons or material interests for ideological or political purposes in order to achieve those goals by means of terror, intimidation or threats. This includes the process of radicalisation.[26]

Article 137 of the Belgian Criminal Code defines terrorism as a list of criminal acts that by their nature or context can significantly harm a country or an international organisation and which was committed with the intent to terrorise the population or to illegitimately compel a government or an international organisation to perform a certain act or to refrain from it, or to seriously destabilise or destroy the political, constitutional, economical or social structures of a country or international organisation. Besides the elaborate scope of Article 137 as opposed to the 1998 Consolidated Act, what stands out is the explicit mention of the process of radicalisation in the latter. Radicalisation is not mentioned in the Belgian Criminal Code. However, this does not mean that it does not fall within the competence of the Federal police. Radicalisation processes are viewed as a preliminary stage of terrorism and thus fall within the prevention task of the federal and local police authorities.[27] The reason why the radicalisation process is included in the definition of terrorism in the 1998 Consolidated Act turns out to be rather technical. Because the radicalisation process was not mentioned anywhere else except in the title covering extraordinary investigative methods, the BIM Commission (cf infra) expressed concern that this would be falsely interpreted as being that these methods were only allowed for the purpose

---

[24] *Van Laethem*, 2 EJIS 5 (2008).

[25] Ibid., 6.

[26] Article 8, 1°, b) of the 1998 Consolidated Act.

[27] See Ministerial Circular GPI 78 of 31 January 2014 on information processing for the purpose of an integrated approach by police authorities of terrorism and violent radicalisation, B.S. 17 February 2014.

of investigating the radicalisation of an individual. In response to this concern, the option was chosen to include radicalisation in the terrorism definition.[28]

The 1998 Consolidated Act, together with the 2003 introduction of legal provisions in the Belgian Criminal Code criminalising the act of terrorism,[29] resulted in a thinning line between police work and intelligence work in the Belgian landscape.[30] This implies that both authorities can be investigating the same criminal acts or individuals. When this parallel effort goes undetected and information is not shared, this may result in a duplication of work – but more importantly, crucial information and connections between bits of information may be missed. The parliamentary commission investigating the circumstances of the 2016 Brussels attacks concluded that a culture shift is necessary in the police and intelligence landscape from the "need to know" principle to the "need to share" principle, while finding the balance between the need for security, the protection of sources, the protection of privacy and the efficiency of investigation and security measures.[31] The commission recommended the removal of obstacles for information sharing and the development of integrated data management and coordination between the competent authorities.[32] Still, Belgium is holding onto the position that intelligence services and police authorities should be separated. According to one scholar, democratic theory and the need to control intelligence services are essential factors in keeping the latter separate from the police.[33]

A particular competence that is not shared with police authorities is the gathering, analysing and processing of intelligence in relation to the activities of foreign intelligence authorities on Belgian territory. In accordance with Article 18/1 of the 1998 Consolidated Act, the specific investigative methods mentioned in that Act (see further in this report) can be used for the purpose of checking[34] foreign intelligence activities on Belgian territory.

---

[28] Chambre, 2043/001, Legislative proposal for amending the law of 30 November 1998 on the organisation of the intelligence and security service and of Article 259 bis of the Criminal Code, travaux préparatoires, 20 September 2016, p. 30.

[29] Act of 19 December 2003 on Acts of Terrorism, B.S. 29 December 2003.

[30] *Van Laethem*, 2 EJIS 3 (2008).

[31] Activity Report State Security Service 2017–2018, p. 8 and Chambre, 1752/008, Parliamentary Investigation into the circumstances that led to the terrorist attacks of 22 March 2016 in Zaventem airport and in metrostation Maalbeek, Brussels including the evolution and the handling of the fight against radicalism and terrorist threats, Third Interim Report on "Security Architecture", 15 June 2017, p. 254.

[32] Ibid., p. 258.

[33] *Matthijs*, 23 Intelligence and National Security 570–571 (2008).

[34] The original text read "assessing the legality of activities of foreign intelligence authorities" but after the advice by Standing Committee I the wording was changed, since assessing legality is a task for the judiciary. See Chambre, 0553/005, Legislative proposal for amending the Act of 30 November 1998 on the intelligence and security authorities

V. Accountability and Investigative Methods

The threefold organisation of investigative methods at the disposal of the intelligence authorities is linked to an important distinction in oversight or accountability. For that reason, the organisation of oversight of the investigative methods is studied first before turning our focus to the investigative methods as such. The 1998 Consolidated Act distinguishes three levels of investigative methods to be used by intelligence authorities: ordinary, specific and extraordinary investigative methods. The distinction is based on the seriousness of the threat and on the fundamental rights breach that using the particular investigative method can cause.

Oversight of the activities of the Belgian State Security Service is organised in a predominantly external manner.[35] Internal supervision is limited to the head of the department authorising *ex ante* the use of investigative methods. The main focus of this section will be on the external supervisory mechanisms.

A. Two oversight bodies

Oversight of the functions of the Federal police and the State Security Service is split into two separate oversight bodies. The supervision of the Federal police lies in the hands of the Standing Police Monitoring Committee (Standing Committee P), whereas the Standing Intelligence Agencies Review Committee (Standing Committee I) carries out the oversight of intelligence activities.[36]

An administrative commission – the BIM Commission (see next subsection) – and a jurisdictional body – Standing Committee I – monitor the activities of intelligence authorities. Both work simultaneously but separately at checking the appropriate use of investigative methods. Since both bodies are similar in composition, competences and working methods, this section will emphasise what differentiates them.

1. BIM Commission

The administrative commission – referred to as the BIM Commission[37] after the Dutch name *Bijzondere Inlichtingenmethoden Commissie* – tasked with monitoring the specific and extraordinary information gathering methods by the intelligence

---

regarding the supervision of the activities of foreign intelligence authorities in Belgium, 14 January 2016, p. 4.

[35] *Van Laethem*, 2 EJIS 22–23 (2008).

[36] Act of 18 July 1991 on the organisation of oversight of police and intelligence agencies and the coordinating body for threat analysis, B.S. 26 July 1991.

[37] See Article 1 of the Internal regulations of the administrative commission tasked with monitoring the specific and extraordinary methods for the gathering of data by intelligence and security authorities (BIM Commission), B.S. 27 September 2016.

authorities is a permanent commission. In carrying out this duty, the commission operates fully independently.[38] All members are magistrates. It is important that in the five years prior to their appointment, no member should have been a member of Standing Committee P monitoring the police authorities, or of Standing Committee I, a police authority, intelligence or security agency.[39]

The BIM Commission has the task of receiving and assessing draft authorisations for the use of extraordinary investigative measures. The members of the commission assess the legality, proportionality and subsidiarity of the measures.[40] Authorisations are granted by unanimous advice from the BIM Commission for a maximum duration of two months, with a possible extension of another two months. Any further extensions are only allowed under special circumstances.[41] Negative advice by the BIM Commission stops the procedure as there is no opportunity for appeal.

The advice of the BIM Commission can be substituted by a different kind of authorisation in two instances. First, if the BIM Commission does not reach a conclusion within four days, the authorisation of the competent Minister shall be sought. The investigative measure should be terminated when the threat is no longer present or when the measure is no longer necessary. The 1998 Consolidated Act, however, does not contain an ultimate maximum duration. Second, in urgent cases the head of the relevant intelligence authority may seek oral authorisation of the chair of the BIM Commission. In the latter case, the investigative measure may only be authorised for a maximum duration of five days.

2. Standing Committee I

Like the BIM Commission, Standing Committee I consists of three effective members, but for each of these, two substitute members are appointed. However, the Chamber – not the King – appoints all members. Each member should not be a member of Committee P, a police authority, intelligence or security authority, the OCAD or a support service thereof, a data protection authority or the aforementioned BIM Commission.[42]

The principal task of Standing Committee I is the *ex post* oversight of the use of specific and extraordinary investigative methods. This duty of oversight consists of several layers. First, the intelligence authorities have an obligation to inform Standing Committee I of any use of the specific and extraordinary investigative methods, the advice given by the BIM Commission and the decisions taken by the latter on

---

38 Article 43/1 of the 1998 Consolidated Act.

39 Article 43/1 of the 1998 Consolidated Act.

40 *De Hert* and *Decaigny*, 1 Ad Rem 27 (2009).

41 Article 18/10 of the 1998 Consolidated Act.

42 Article 28 of the Act of 18 July 1991, B.S. 26 July 1991.

terminating the investigative methods. Second, Standing Committee I can be charged to assess the legality of the use of both specific and extraordinary investigative methods by any citizen who can demonstrate a personal and legitimate interest, by the Belgian Data Protection Authority or it can act *ex officio*.[43] Third, the committee investigates every case in which the competent Minister has intervened due to inaction of the BIM Commission and every case of suspension by the BIM Commission of the illegal use of an investigative method.[44]

In order to fulfil its duties, Standing Committee I is supported by an administrative department and the department of investigations (*Dienst Enquêtes I*).[45] At least half of the members of the department of investigations are seconded from police or intelligence authorities or an administration where they gained at least five years of experience with the activities of police and intelligence authorities. This is thus a different approach in comparison to the above-mentioned members of Standing Committee I itself. Moreover, the members of the department of investigations are given the capacity of "judicial police, deputy officer of the prosecutor".[46] This means that they have the competence to conduct searches, confiscate goods and order the production of documents. They have the task of checking whether members of the intelligence authorities commit criminal acts – with the exception of acts committed in undercover operations – in the carrying out of their duties and they initiate investigations in that respect, in which case Standing Committee I should be informed.[47]

B. Investigative Methods

The original 1998 Act that governed the Belgian intelligence and security services[48] lacked strong investigative methods. In order to fulfil its task of gathering, analysing and processing intelligence, the State Security Service was limited to the use of human intelligence, the actual collection of data and the exchange of information with other authorities.[49] This was considered insufficient to counter the increasing threat of – amongst others – terrorism and extremism. An additional argument made in the *travaux préparatoires* is that the State Security Service is supposed to feed the threat assessment body OCAD with their analyses whereas the federal police and the customs authorities – who are also partners within OCAD – had more

---

[43] *De Hert* and *Decaigny*, 1 Ad Rem 28 (2009) and Article 43/4 of the Act of 18 July 1991, B.S. 26 July 1991.

[44] Article 43/4 of the Act of 18 July 1991.

[45] *Van Laethem*, 2 EJIS 23 (2008).

[46] Article 45 of the Act of 18 July 1991.

[47] Article 45 of the Act of 18 July 1991 and *Van Laethem*, 2 EJIS 23 (2008).

[48] Act of 30 November 1998 on intelligence and security services, B.S., 18 December 1998.

[49] Senate, Travaux Préparatoires 3-2138/1, 2006, p. 9.

powerful tools to work with.[50] For these reasons, the Belgian legislator considered it necessary to provide the State Security Service with the so-called specific and extraordinary investigative methods. The latter two are distinguished based on the threat and the fundamental rights breach for the individual who is the subject of the investigation. Guiding principles are subsidiarity and proportionality as well as sufficient guarantees against any possible abuse.

A crucial factor in the revision of the 1998 Consolidated Act was the arguments raised by the defence counsel of one of the suspects in the so-called GICM trial. During the trial against suspected members of the *Groupe islamique combattant marocain* (GICM) a defence attorney raised questions regarding the supervision and infringements of the privacy of his client by the State Security Service when it gathered important phone numbers via informants. Even when in this particular case the defendants were sentenced for their share in a terrorist group, the judges of the Brussels Correctional Tribunal gave a clear signal to the legislator that the legal framework – in particular the 1998 Act – was in dire need of revision.[51]

Remarkably, the *travaux préparatoires* mention that the specific and extraordinary investigative methods inserted into the 1998 Consolidated Act in 2010 are similar to those provided to police authorities, but still the inspiration for these legal provisions came from the 2002 Dutch law on methods for the collection of data by intelligence services. The reason for this look across the border was the fact that the Dutch law contains a stronger consideration for the purpose of the work of intelligence authorities.[52]

A specific investigative method may only be used when ordinary investigative methods are deemed insufficient. Similarly, when the specific investigative methods are deemed insufficient then extraordinary investigative methods may be used. As highlighted by De Hert and Decaigny, the distinction between ordinary, specific and extraordinary investigative methods is only partially subsidiary; an important difference is also made in the level of oversight.[53]

The following sections zoom in on each category and include the organisation of oversight per category with references where relevant to a separate section dedicated to oversight further in this report. The investigative methods used by intelligence authorities are divided in different categories – ordinary, specific and extraordinary methods – in comparison to the police authorities' investigative methods – ordinary and special methods. This section is organised based on the intelligence authorities' categories of investigative methods. A separate subsection is dedicated to the special

---

[50] Senate, Travaux Préparatoires 3-2138/1, 2006, p. 10.

[51] Senate, Travaux Préparatoires 3-2138/1, 2006, p. 6–7 and Cour d'Appel Brussels 19 January 2007 and Cour de Cassation, 27 June 2007. See also *De Hert* and *Decaigny*, 1 Ad Rem 24 (2009).

[52] Ibid., p. 15.

[53] *De Hert* and *Decaigny*, 1 Ad Rem 26 (2009).

investigative methods that can only be used by police authorities and not by intelligence authorities.

1. General

The use of coercive measures by intelligence authorities is only allowed under the conditions imposed by law.[54] This principle is in essence not different from the principle that applies to police authorities. The latter can act under the direction of the locally competent prosecutor in criminal investigations as long as no coercive measures are used. Once coercive measures such as a house search or arrest are necessary for the purpose of the investigation, an investigative judge (*onderzoeksrechter*) needs to authorise use of the measure. The Belgian Code of Criminal Procedure therefore distinguishes a police investigation (*opsporingsonderzoek*) where a prosecutor has the lead and there is no need for coercive measures from a judicial investigation or (*gerechtelijk onderzoek*) which is led by the investigative judge.[55]

2. Ordinary investigative methods

Ordinary investigative methods include the gathering of information without technical means or by receiving them from another authority, private company or person. Introducing such a way of working implies introducing an obligation for the national public and judicial authorities to transfer information when necessary for the purpose of an investigation. Refusal to hand over the requested information remains a possibility when this would hinder an on-going judicial or police investigation, an on-going gathering of information in the context of money laundering and the financing of terrorism, or when it could significantly infringe upon a person's privacy. It should be mentioned that the 1998 Consolidated Act also includes the spontaneous transfer of relevant information by public service officials and police authorities to intelligence authorities.[56]

Without the use of technical means, intelligence authorities can observe people, objects and events or incidents in locations that are accessible to the public. The interpretation of "locations that are accessible to the public" led to confusion concerning private places that are still accessible to the public. For that reason, a 2017 amendment to the 1998 Consolidated Act inserted an additional definition into the law's third article. A distinction is now made between, on the one hand, those locations that are either public or private but accessible to the public and, on the other hand, those locations that are visible to the public but not publicly accessible. The latter is defined as publicly inaccessible locations that are visible from the public

---

[54] Article 12 of the 1998 Consolidated Act.

[55] See Articles 28 bis and following of the Code of Criminal Procedure.

[56] Article 14 of the 1998 Consolidated Act.

street without technical assistance or manipulation. Once a ladder or drone would be necessary for the observation, the location no longer falls within the scope of ordinary investigative methods. The described distinction becomes relevant where observation of individuals who are on a public street and then step onto the private driveway of a home is concerned. Before the additional definition was inserted in the law, an individual walking on a street could be watched by means of the ordinary observation method, but the intelligence officer who wished to continue observing the individual once the latter had stepped onto a private driveway (considered an attachment of the home and hence falling under the reasonable expectation of privacy) should request an extraordinary observation. In order to avoid such a surreal situation, the above-described definition ensures that even private places that are accessible to the public can be observed as an ordinary investigative method. Thus, intelligence authorities do not need authorisation for these types of observation.[57]

There is a difference in this respect with the competences of police authorities. In the context of a police investigation lead by the locally competent prosecutor, the latter needs to authorise police authorities to enter[58] (without permission or knowledge of the rightful owner) private property that is not a home or an attachment to a home such as driveways, gardens, etc.[59] When a home or its attachments are involved, an investigative judge should authorise the observation or search in the context of a judicial investigation.[60] No distinction is made here based on whether or not a private place is accessible to the public or visible from the public street.

The Belgian Code of Criminal Procedure makes an important distinction between, on the one hand, the simple observation as described in the previous paragraph and, on the other hand, observation as a special investigative method by police authorities. The latter is called a systematic observation, defined as either an observation with duration of more than five consecutive days (or five non-consecutive days within one month), an observation with the help of technical means, a cross-border observation or an observation carried out by special units of the federal police.[61] Observations with the help of technical means are only allowed for criminal offences punishable by one or more years of imprisonment. The other types of systematic observation by police authorities are not restricted by such threshold, however the use of it should always fulfil the requirements of necessity and proportionality. The prosecutor's power to authorise a systematic observation ends when the location to

---

[57] Chambre, 2043/001, Legislative proposal for amending the law of 30 November 1998 on the organisation of the intelligence and security service and of Article 259 bis of the Criminal Code, Travaux Préparatoires, 20 September 2016, p. 28.

[58] The use of technical means is considered equivalent to entering in accordance with Article 46 quinquies §4 of the Code of Criminal Procedure.

[59] Article 46 quinquies §1 of the Code of Criminal Procedure and Articles 479 to 481 of the Criminal Code.

[60] Article 56 bis and Article 89 ter of the Code of Criminal Procedure.

[61] Article 47 sexies of the Code of Criminal Procedure.

be observed is a home or the attachments to a home. In these circumstances the investigative judge should authorise the measure.[62]

In accordance with Article 16/2 and 16/3 of the 1998 Consolidated Act, intelligence authorities can request information from private companies, such as operators of electronic communication networks or providers of electronic communication services and banks or financial institutions. Requests for cooperation from the telecommunication operators and providers should however be restricted to identifying the subscriber or identifying the service and means by which an individual is subscribed or which are typically used by a specific individual. Thus the content of communications does not fall within the scope of ordinary investigative methods. This is similar to the competences in the context of a police investigation led by the locally competent prosecutor. In accordance with Article 46bis of the Code of Criminal Procedure, the prosecutor can demand information identifying the subscriber or identifying the service, but not the content of the communications. Where criminal offences punishable with imprisonment of one or more years are concerned, the investigative judge can not only order traffic data of electronic communications and the localisation of their origin and destination[63] but can also order the cooperation of anyone – with the exception of the suspect – who has knowledge of the security or encryption of an IT system in order to gain access to data.[64] Further, the investigative judge has far-reaching competences to penetrate an IT system in order to gain access to data or even install technical means in the IT system. The latter is a measure only allowed for a list of serious criminal offences.[65]

Intelligence authorities can demand cooperation from banks or financial institutions in order to identify an end-user of a prepaid electronic communication. Police authorities, in the context of a police investigation led by the locally competent prosecutor, can do this as well, although they operate under stricter limitations. Information on bank accounts and transactions within a specific timeframe can be requested for criminal offences punishable by imprisonment of one or more years. If necessary the prosecutor can also monitor bank transactions for a renewable maximum duration of two months. An additional restriction is applicable for less serious criminal offences, i.e. those offences that are punishable with imprisonment for less than one year. In such cases the prosecutor can only demand the identifying information for a period of six months prior to the authorisation. If a serious criminal offence is concerned, as listed in Article 90 ter §2 to 4 of the Code of Criminal Procedure, the prosecutor can block bank accounts for a maximum of five working days.

---

62 Article 56 bis and Article 89 ter of the Code of Criminal Procedure.

63 Article 88 bis §1 of the Code of Criminal Procedure.

64 Article 88 quater of the Code of Criminal Procedure.

65 Article 90 ter of the Code of Criminal Procedure.

In accordance with Article 16/3 of the 1998 Consolidated Act and given the processing of passenger name records enacted by law in 2016, intelligence authorities are allowed to have access to passenger data for the purpose of their investigations. Whereas intelligence authorities are granted access to these data, police authorities are restricted to ordering specific data. More precisely, police authorities acting in the context of a police investigation led by the locally competent prosecutor can order the transfer of passenger name records from the Passengers Information Unit. This order can only be made for the purpose of investigating a serious criminal offence as listed in Article 90 ter of the Code of Criminal Procedure, in addition to several offences of forgery, piracy and counterfeiting.[66]

3. Specific investigative methods

Specific investigative methods are those methods that can be used when ordinary investigative methods are deemed insufficient to gather the information necessary for completing the task. Specific methods thus include: observation of public places with technical means; observation and search of private places accessible to the public with or without technical means; receiving the identity of the sender of mail or the subscriber of an electronic mail service and traffic data of electronic communications.[67] In 2017 an additional provision was inserted in the 1998 Consolidated Act also giving intelligence authorities the power to claim passengers' travel data from private companies providing transport or travel services.[68]

The procedural requirements for using the specific investigative methods are rather slim in comparison to similar investigative methods used by police authorities. For example, De Hert and Decaigny[69] rightfully point out that observation as a specific investigative method by intelligence authorities is not restricted in time, as is the case for systematic observation by police authorities in accordance with Article 47 sexies of the Criminal Procedure Code. Moreover, observation by technical means by police authorities is only allowed for criminal offences punishable with at least one year of imprisonment. The 1998 Consolidated Act does not contain such a threshold. Where the competent investigative judge maintains oversight over observations carried out by police authorities and authorises observations that breach the privacy of the persons involved, observations by intelligence authorities are authorised by the head of their department. The aforementioned BIM Commission is merely informed, but does not authorise the use of specific investigative methods.

---

[66] Article 46 septies of the Code of Criminal Procedure and Article 8 of the Act of 25 December 2016 on the processing of passenger data, B.S. 25 January 2017.

[67] Articles 18/4 to 18/6 of the 1998 Consolidated Act.

[68] Article 18/6/1 of the 1998 Consolidated Act.

[69] *De Hert* and *Decaigny*, 1 Ad Rem 26 (2009).

4. Extraordinary investigative methods

When specific investigative methods are deemed insufficient, intelligence authorities may turn to extraordinary investigative methods. These are methods that by their nature or effect infringe upon the privacy of the person(s) involved. They include: observation and searches with or without technical means in homes; searches of closed objects located in homes; creating a legal person and use of a fictional identity by officers operating undercover; opening mail; gathering information on bank accounts and transactions; penetrating an IT system with or without technical means, fake signals, fake keys or fake identities and intercepting and recording communications.[70]

Use of extraordinary investigative methods by intelligence authorities is further restricted to: serious threats to a fundamental interest of the country; serious threats related to espionage, terrorism, extremism, proliferation, sectarian organisation or criminal organisations; or the activities of a foreign intelligence service. Due to the clear infringement of privacy rights of the persons involved, *ex ante* oversight is organised in two steps. First, the head of the department of the intelligence authority should draft an authorisation. Second, the BIM Commission examines the draft authorisation on the legality, subsidiarity and proportionality of the investigative method. One of the mandatory sections of the draft authorisation is the mentioning of whether or not the on-going intelligence investigation runs parallel to a police investigation. Remarkably, the 1998 Consolidated Act does not prohibit parallel investigations – it only requires intelligence authorities not to conduct investigations that harm police investigations.[71]

The BIM Commission gives an advice based on the draft authorisation within four days. Moreover, at any moment the commission can exercise its oversight of the use of the extraordinary investigative methods it authorised.

The use of extraordinary investigative methods is restricted in time to a maximum of two months starting from the day of authorisation. The term of two months can be extended once. Further extensions are only possible in extraordinary circumstances. In any case, use of the investigative method should be terminated once the conditions – including the potential threat – that authorised it cease to apply.

The described restrictions and oversight for using extraordinary investigative methods by intelligence authorities are more in line with the use of similar investigative methods by police authorities. The fact that an infringement of privacy is the distinguishing criteria for extraordinary methods implies that these investigative methods can only be carried out by police authorities following the authorisation by

---

[70] Article 13/5 of the 1998 Consolidated Act.

[71] Article 13/5 of the 1998 Consolidated Act. See also *De Hert* and *Decaigny*, 1 Ad Rem 27 (2009).

the investigative judge. An exception is the use of fictional identities, which is a measure that can be authorised by the locally competent prosecutor for investigations into criminal offences punishable with one or more years of imprisonment.[72]

5. Special investigative methods for police use only

The Code of Criminal Procedure contains a subsection dedicated to special investigative methods that contains three types of method that can be ordered by the locally competent prosecutor: systematic observation (see above), infiltration and the use of informants. The Belgian legal framework only allows for infiltration and the use of informants by police authorities.

Infiltration is defined by Article 47 octies of the Code of Criminal Procedure as the sustaining of contacts by a police officer using a fictional identity, with one or more persons who are suspected of committing or have committed serious criminal offences[73] in the context of a criminal organisation. Even though the use of fictional identities is a method used by intelligence authorities in accordance with the 1998 Consolidated Act, the *travaux préparatoires* explicitly state that this does not offer a legal basis for infiltration operations. This restriction originates from the opinions presented by the BIM Commission and Standing Committee I.[74] The reason for this restriction is the difference in purpose of the fictional identity. For intelligence authorities the fictional identity is a protective measure, not a method of information gathering.

Since July 2018, a new special investigative method has been added to the toolbox of Belgian police and prosecution authorities.[75] Besides the infiltration by police officers, as described above, it is now also possible to organise the infiltration of a criminal organisation by a civilian. Civilian infiltration was previously not allowed in Belgium due to the risks such method can entail for the person involved. Logically, infiltration by a civilian is only allowed for investigations into serious offences[76] and following the authorisation by the locally competent prosecutor, investigative judge

---

[72] Article 46 sexies of the Code of Criminal Procedure.

[73] As defined by Articles 90 ter § 2 to 4 of the Code of Criminal Procedure.

[74] See Chambre, 2043/001, Legislative proposal for amending the law of 30 November 1998 on the organisation of the intelligence and security service and of Article 259 bis of the Criminal Code, Travaux Préparatoires, 20 September 2016, p. 12.

[75] Act of 22 July 2018 amending the Code of Criminal Procedure and the Preceding Title to the Code of Criminal Procedure to introduce the special investigative method of civilian infiltration, B.S. 7 August 2018.

[76] As defined by Article 90 ter §2 to 4 of the Code of Criminal Procedure with the exception of specific forms of organised crime, and on the condition that these offences are committed in the context of a terrorist crime.

or federal prosecutor.[77] Infiltration by a civilian is not an investigative method that can be used by intelligence authorities.

Belgian intelligence authorities can rely on human sources for the purpose of gathering information on events, objects, groups and (natural and legal) persons who seem relevant for their investigations.[78] In accordance with Article 47 decies of the Code of Criminal Procedure, police authorities can use informants. This is defined as the maintaining of regular contact by a police officer with an individual who is suspected of having close ties with one or more persons who are suspected of committing or have committed criminal offences, and who – on request or spontaneously – provides the police officer with information. The Code of Criminal Procedure does not provide a threshold for the use of informants, except for allowing the informant to commit offences in order to keep his or her information position. That is only allowed for the purpose of investigations into serious offences listed in Article 47 decies §7.

VI. Joint Police and Intelligence Meetings

There are two instances where the organisation of the Belgian police and intelligence landscape includes joint efforts by the bodies governing police and intelligence authorities: the gathering of information for the purpose of threat analysis and joint meetings of both supervisory committees.

A. Threat analysis

In 2006 the Anti-terrorist Mixed Group – set up in 1984 in the context of the then terrorist threat by the group Cellules Communistes Combatantes – was replaced by the Coordination Organ for Threat Analysis (OCAD).[79] In addition, all staff of the Anti-terrorist Mixed Group were transferred to OCAD. OCAD consists of a director, deputy-director, experts who are seconded by the support services, analysts and support staff. The support services are the intelligence authorities, police authorities, customs authorities, the federal public service of mobility and transport, the federal public service of interior – in particular the service for foreigners – and the federal public service of foreign affairs. Following a proposal by the Ministerial Committee for Intelligence and Security, the King can add other services to this list.[80] For example, by Royal Decree of 17 August 2018, the following services were added to the support services: the general directorate crisis centre, the directorate-general

[77] Article 47 novies of the Code of Criminal Procedure.

[78] Article 18 of the 1998 Consolidated Act.

[79] Act of 10 July 2006 on Threat Analysis, B.S. 20 July 2006.

[80] Article 2 of the Act of 10 July 2006 on Threat Analysis.

penitentiary institutions, the bureau of worship and liberty of the directorate-general legislation, fundamental rights and freedoms, and the general administration of the treasury.[81]

The general task of OCAD is to analyse and assess potential threats based on the information received by the support services. The most significant distinction between OCAD and its predecessor the Anti-terrorist Mixed Group is the mandatory nature of information transfer by the support services.[82] This obligation to share may have been introduced for the purpose of building a better information position; it raised concerns with foreign intelligence authorities fearing an unwanted distribution of their information.[83] The Royal Decree executing the Act on Threat Analysis specified that information can only be included in a threat assessment when the foreign authority who transferred it explicitly agreed to its content, modalities, distribution and degree of classification.[84] In practice – and due to OCAD gaining more traction with foreign intelligence services – foreign intelligence is now shared with the label "for Belgian eyes only".[85] In its report on the circumstances of the 2016 terrorist attacks, the parliamentary commission investigating the Belgian security architecture mentioned that the use of the label "for Belgian eyes only" means that the given intelligence may be used by all Belgian authorities. With the lack of such a label, a restrictive interpretation should be assumed.[86]

B. Joint meetings of Standing Committees I and P

At least twice per year the Standing Intelligence Agencies Review Committee (Standing Committee I) and the Standing Police Monitoring Committee (Committee P) have a joint meeting with alternating presidency. Originally, these meetings were dedicated to cooperation in order to set up the functioning of both committees due to a lack of infrastructure and staff. This meant that in 1993 and 1994 a total of 16 joint meetings were held discussing issues such as internal regulations, status of staff and

---

[81] Royal Decree of 17 August 2018 in execution of Article 2, §1, 2°, g) of the Act of 10 July 2006 on Threat Analysis, B.S. 12 September 2018.

[82] Article 6 of the Act of 10 July 2006 on Threat Analysis.

[83] *Lasoen*, 30 International Journal of Intelligence and Counterintelligence 474 (2017).

[84] Article 15 of the Royal Decree of 28 November 2006 executing the Act of 10 July 2006 on Threat Analysis, B.S. 1 December 2006. See also *K. Lasoen*, For Belgian Eyes Only, International Journal of Intelligence and Counterintelligence, Vol. 30, Nr. 3, 2017, p. 474.

[85] *Lasoen*, 30 International Journal of Intelligence and Counterintelligence 475 (2017) and Activity Report Standing Committee I, Intersentia, 2011, p. 29.

[86] Chambre, 1752/008, Parliamentary Investigation into the circumstances that led to the terrorist attacks of 22 March 2016 in Zaventem airport and in metrostation Maalbeek, Brussels including the evolution and the handling of the fight against radicalism and terrorist threats, Third Interim Report on "Security Architecture", 15 June 2017, p. 471.

security of the building.[87] Now, these meetings are organised for two purposes: to exchange information and to start and discuss running common oversight investigations.[88]

Exchanging information does not include operational information or intelligence; rather, it refers to information on oversight activities, activity reports and decisions. Committees I and P bear common oversight responsibilities with regard to those agencies that have both police and intelligence tasks, such as the aforementioned OCAD. Common oversight can be organised with regard to OCAD, such as its information position on the eve of the terrorist attacks in Paris of 13 November 2015.[89]

Furthermore, the joint meetings of both committees are used for coordinating the functioning of the police and intelligence authorities as well as any other issue that may be brought to them by the competent Minister or the Chamber of Representatives.[90]

VII. Transfer of Information

The cooperation between authorities in transferring relevant operational information is divided into two branches: cooperation between intelligence authorities, police and prosecution authorities on a national level on the one hand, and the cooperation between the intelligence authorities of Belgium and foreign intelligence authorities on the other.

A. Cooperation on a national level

It is the task of the State Security Service to detect at an early stage those aspects that could instigate specific individuals to actions that could potentially be a threat and could be violent even when they may not seem a threat or violent at first sight.[91] When the use of specific or extraordinary investigative methods reveals significant indications or presumptions that offences are or will be committed, the intelligence authorities have the obligation to transfer this information to the BIM Commission immediately. This obligation fits within the general duty for every public official

---

87 Activity Report Standing Committee I, 1994, p. 54.

88 Activity Report Standing Committee I, Intersentia, 2017, p. 96.

89 Activity Report Standing Committee I, Intersentia, 2017, p. 96–97.

90 Article 53 of the Act of 18 July 1991.

91 Act amending the Act of 30 November 1998 on the Intelligence and Security Services and of Article 259 bis of the Criminal Code, Travaux Préparatoires 2043/001, 20 September 2016, p. 5.

who is made aware of the commission of an offence in the exercising of his or her tasks, to instantly inform the locally competent prosecutor.[92]

The BIM Commission, however, is an important filter in this respect. When the Commission concludes on the existence of significant indications of an offence that will be committed or a reasonable suspicion that an offence has been committed but not yet discovered, the chair will draw up a report (*proces-verbaal*) that will be sent to the locally competent prosecutor or the federal prosecutor.[93] This report may never be the exclusive ground, nor can it be the determining measure, on which any person is convicted of an offence. There should always be other evidential material to that end.[94]

Scholars such as Van Laethem rightfully point out that there is a significant overlap between the mandate of intelligence authorities and that of police and prosecution authorities. Especially with regard to terrorism and extremism, judicial authorities in Belgium have been able to undertake preliminary studies to determine whether they can start a proactive investigation into actions that could possibly be classified as preparation for certain crimes or attempts to this end.[95] What Van Laethem means to say is that the closer examination of phenomena that are not (yet) incorporated into punishable behaviour in the legal framework of the Criminal Code, such as radicalisation, is very close to intelligence work.

The 1998 Consolidated Act stipulates an efficient mutual cooperation between intelligence and security authorities, police authorities, administrative and prosecution authorities.[96] For that purpose, intelligence authorities can assist and in particular deliver technical assistance to judicial and administrative authorities, but only on request. Spontaneous assistance is not allowed. The details of this cooperation between the State Security Service, the General Service for Intelligence and Security and the prosecution authorities were laid down in a confidential joint circular adopted in 2005.

B. Cooperation with foreign intelligence authorities

Only one sentence in the 1998 Consolidated Act refers to cooperation: the intelligence and security authorities will make sure there is cooperation with foreign intelligence and security authorities.[97] Information received from foreign counterparts is

---

92 Article 29 of the Code of Criminal Procedure.

93 Article 19/1 of the 1998 Consolidated Act.

94 Article 19/1 of the 1998 Consolidated Act.

95 *Van Laethem*, 2 EJIS 3–4 (2008).

96 Article 20 §1 of the 1998 Consolidated Act.

97 Article 20 §1 of the 1998 Consolidated Act.

usually dealt with under the "third party rule",[98] meaning that the authority that provided the information should give its consent to further distributing the information. In practice this raised difficulties for feeding the threat analysis unit OCAD, which was solved by introducing the label mentioned above, "for Belgian eyes only".

VIII. Concluding Remarks

In general a gradual widening of Belgian intelligence authorities' competences can be seen in the past two decades. Inspired by foreign legislation as well as terrorist attacks on Belgian and French territory, a series of amendments were made to the 1998 Consolidated Act and relevant other legislative acts and royal decrees.

Even when Belgian legal provisions do not prohibit parallel investigations conducted by intelligence and police authorities into the same criminal acts, a filter on exchanging information between both types of investigation is established in the shape of the BIM Commission consisting of magistrates. The different purpose of both investigations – protecting the country from specific threats for intelligence authorities and preventing and investigating criminal acts for police authorities – give rise to the delineation of both authorities' mandate. The latter is defined in terms of the criminal acts, which for intelligence authorities is more restricted than for police authorities. However, both mandates overlap in some areas of crime, in particular with regard to terrorism.

A remarkable evolution in Belgium is the joining of intelligence authorities and police authorities in specific oversight functions and in the flow of information to the threat analysis unit OCAD. Some concern remains among scholars regarding the lack of clear rules for intelligence authorities and the use of different thresholds for particularly intrusive investigative methods. On 1 March 2019, the Council of Ministers approved a new proposal for a royal decree that should amend the royal decree of 12 October 2010 executing the 1998 Consolidated Act. The text of the proposal was not yet published at the time of preparing this report; however it was announced to include – among other things – specific rules on access rights for intelligence authorities to the data gathered by police cameras.[99] This demonstrates the still ongoing modifications to the current legal framework and the toolbox of Belgian intelligence authorities.

---

[98] *Van Laethem*, 2 EJIS 17 (2008) and *Lasoen*, 30 International Journal of Intelligence and Counterintelligence 474 (2017).

[99] Council of Ministers, Press Release, 1 March 2019.

References

De Hert, Paul and *Decaigny, Tom*, De Wet bijzondere methoden inlichtingen- en veiligheidsdiensten (BIM) – Het perspectief van de rechten van de verdediging, 1 Ad Rem 24 (2009).

Eijkman, Quirine and *Van Ginkel, Bibi,* Compatible or Incompatible? Intelligence and Human Rights in Terrorist Trials, Expert Meeting Paper, International Centre for Counter-Terrorism (2011).

Jacques, Laura and *Van Caeneghem, Jozefien*, Monthly data collection on the current reform of intelligence legislation – Belgium, Milieu Ltd (2017)

Lasoen, Kenneth L., For Belgian Eyes Only, 30 International Journal of Intelligence and Counterintelligence 464 (2017)

Lasoen, Kenneth L., Belgian Intelligence SIGINT Operations, 32 International Journal of Intelligence and Counterintelligence 1 (2019)

Lefebvre, Stéphane, 30 "The Belgians Just Aren't up to It": Belgian Intelligence and Contemporary Terrorism, International Journal of Intelligence and Counterintelligence, 1 (2017)

Leroy, *Patrick,* La communauté du renseignement belge – Essai de définition, 12 Revue militaire belge 85 (2016).

Matthijs, *Herman*, Intelligence Services in Belgium, 23 Intelligence and National Security 552 (2008)

Van Laethem, *Wouter,* The Belgian Civil Intelligence Service: Roles, Powers, Organisation and Supervision, 2 EJIS 1 (2008).

Verbrechensbekämpfung durch Nachrichtendienste in Bulgarien

Kamen Lyubomirov Novikov

I. Einleitung

Seit dem Sturz des sozialistischen Regimes in Bulgarien im November 1989 befinden sich sämtliche staatlichen Institutionen in einer Phase der ständigen Reformen auf allen Ebenen. Bei diesen umfangreichen Prozessen stellen die Nachrichtendienste natürlich keine Ausnahme dar. Ihre Entwicklung nach 1989 können wir in drei Hauptperioden unterteilen:

Die erste Periode dauerte bis Juli 1991. In dieser Anfangsphase funktionierte das Sicherheitssystem absolut chaotisch – unter neuen sozialen und politischen Bedingungen, aber auf der Basis der sozialistischen Verfassung und Gesetzgebung. In dieser Periode waren die Nachrichtendienste praktisch blockiert und konnten ihre Aufgaben kaum erfüllen.

Am 13. Juli 1991 trat die neue demokratische Verfassung Bulgariens in Kraft. Damit begann die zweite Periode in der Entwicklung der Nachrichtendienste. Diese Verfassung ist bis heute aktuell, obwohl viele Experten der Meinung sind, dass eine grundsätzliche Änderung der Verfassung mehr als notwendig ist. In dieser zweiten Periode begann der institutionelle Aufbau der Nachrichtendienste auf allen Ebenen (Gesetzgebung, Organisation, technische Ausrüstung und Personal). Schaut man sich die Neuaufbauphase genauer an, so lässt sich vorab konstatieren, dass diese Prozesse langsam, oft konzeptlos und sehr umstritten durchgeführt wurden. Sehr häufig waren die politischen, anstatt der sachlichen und fachlichen Argumente an erster Stelle. Die zweite Periode endete am 1. Januar 2007, als Bulgarien ein Vollmitglied der EU wurde.

Die dritte Hauptperiode begann 2007. Die Nachrichtendienste stehen nun vor völlig neuen Herausforderungen: Harmonisierung der Rechtsvorschriften mit den internationalen Regelwerken, effektiver Schutz der Grundrechte und das in einer komplexen Situation der zunehmenden Kriminalität mit neuen, bisher unbekannten Erscheinungen.

II. Organisation der Sicherheitsbehörden

Die Sicherheitsarchitektur von Bulgarien besteht aus verschiedenen Staatsbehörden, die nachrichtendienstliche, operativ-präventive, strafverfolgende Funktionen ausüben. Die entsprechenden Dienste

- agieren in ständiger Koordination miteinander,
- werden unterstützt von allen staatlichen und lokalen Behörden, von juristischen Personen und einzelnen Bürgern, und
- arbeiten mit Sicherheitsorganen aus anderen Ländern Europas und weltweit eng zusammen.

Die Organisation und Funktion der nationalen Sicherheitsarchitektur Bulgariens sind in der Verfassung und in speziellen Gesetzen geregelt. Dessen Grundprinzipien sind:

- Beachtung der Gesetze und der internationalen Regelwerke,
- Politische Neutralität,
- Beachtung der Grundrechte der Bürger,
- Objektivität und Unparteilichkeit,
- Kooperation mit anderen Staatsorganen,
- Offenheit und Verantwortung bei der Gestaltung der Sicherheitspolitik,
- Zentralisierte Leitung und Kontrolle der nachrichterdienstlichen Tätigkeit,
- Schutz der Daten und der Informationsquellen, und
- Informationsaustausch mit den anderen staatlichen Behörden.

Nach der derzeitigen Gesetzgebung und gemäß dem Grundprinzip der Gewaltenteilung üben die Legislative, die Exekutive und die Judikative ihren Einfluss auf die Nachrichtendienste aus. Die Beteiligung der drei Gewalten an der nationalen Sicherheitsarchitektur Bulgariens soll eine Garantie gegen Monopol und Machtkonzentration in den Sicherheitseinheiten sein.

Das Parlament ist zwar nicht direkt an der Arbeit der Nachrichtendienste beteiligt, aber dessen Aktivität auf der Ebene der Gesetzgebung ist grundlegend für die Einrichtung und Funktion aller staatlichen Behörden. Außerdem verabschiedet das Parlament jährlich das Budget der Sicherheitsorgane – eine sehr wichtige Frage und eine Hauptvoraussetzung für die Effektivität der Nachrichtendienste. Genannt werden müssen auch die verschiedenen Parlamentsausschüsse, die Zugang zu nachrichtendienstlichen Information haben und Kontrollbefugnisse ausüben.

Die Regierung führt und realisiert die Innen- und Außenpolitik des Staates. Dass sie im Bereich der nationalen Sicherheit bestimmend ist, ist unumstritten. Die meisten Behörden mit nachrichtendienstlichen Funktionen in Bulgarien sind Teil der Exekutive und sind dem Premierminister und den verschiedenen zuständigen Ministern unterstellt.

Die Regierung führt den Sicherheitsrat, der die Arbeit der Nachrichtendienste ständig kontrolliert, koordiniert und analysiert. Mitglieder des Sicherheitsrats sind der Premierminister, der Minister für Europäische Politik, die stellvertretenden Premierminister, der Innenminister, der Außenminister, der Finanzminister, der Verteidigungsminister, der Stabschef der Armee und der Leiter aller Nachrichtendienste.

Die Organisation und Struktur des Justizsystems sind in der Verfassung und im Gesetz für die richterliche Gewalt[1] geregelt. Die richterliche Gewalt in Bulgarien wird von den Gerichten, der Staatsanwaltschaft und dem Ermittlungsamt verkörpert. Die Staatsanwaltschaft ist eine Strafverfolgungsbehörde; verfassungsrechtlich gehört sie zur Judikative, und nicht zu der Exekutive, wie es etwa in Deutschland, Belgien, Irland, Finnland, Norwegen oder Polen der Fall ist.

In einem eingeleiteten Ermittlungsverfahren laufen die Ermittlungen unter der Leitung und Aufsicht der Staatsanwaltschaft. Art. 194 der Strafprozessordnung bestimmt, in welchen Fällen Ermittler tätig werden. In diesem Zusammenhang gilt der Grundsatz, dass sie Strafsachen mit hohem sachlichen und rechtlichen Schwierigkeitsgrad untersuchen.

Eine sehr wichtige Rolle bei der Organisation und Funktion der Sicherheitsbehörden in Bulgarien spielt der Präsident der Republik. Er ist das Staatsoberhaupt, der oberste Befehlshaber der Streitkräfte und steht verfassungsrechtlich außerhalb des Systems der drei Gewalten.

---

[1] Amtsblatt № 64/07.08.2007, https://www.lex.bg/laws/ldoc/2135560660.

Der Präsident ist zugleich Vorsitzender des Rates für die Nationale Sicherheit. Mitglieder dieses Rates sind der Premierminister, der Parlamentspräsident, der Innenminister, der Außenminister, der Finanzminister, der Verteidigungsminister, der Stabschef der Armee und Vertreter aller im Parlament vertretenen Parteien. Der Rat für die Nationale Sicherheit analysiert die innen- und außenpolitische Lage und trifft Entscheidungen in Krisensituationen, garantiert den Frieden, die öffentliche Ordnung und die Grundrechte der Bürger, reagiert bei Gefahr für den Staat. Außer seiner Arbeit im Rat für die Nationale Sicherheit stehen dem Präsidenten wichtige Befugnisse innerhalb der Sicherheitsarchitektur zu. Er nimmt an Personalernennungen der Nachrichtendienste teil und verfügt über das Vetorecht bei fast allen Entscheidungen der Exekutive, die die Sicherheit des Staates betreffen.

III. Sicherheitsbehördliche Aufgabenfelder

In Bulgarien besteht keine *klare* funktionale Aufteilung der Aufgabenfelder zwischen den Nachrichtendiensten, Polizei und Staatsanwaltschaft. Die Nachrichtendienste sind zwar informationssammelnd-präventiv ausgerichtet, haben aber auch Befugnisse in der Strafverfolgung. Die Polizei betreibt sowohl operative Prävention als auch die Strafverfolgung. Ist ein Ermittlungsverfahren bereits eingeleitet, so ist ausschließlich die Staatsanwaltschaft zuständig und hat unumstritten die führende Rolle.

A. Nachrichtendienste

Die Nachrichtendienste in Bulgarien sind innerhalb der exekutiven Gewalt angesiedelt. Die Dienste sind selbstständige Einheiten mit eigenem Rechtsrahmen, eigener Verwaltung und eigenen Befugnissen.

Zurzeit des sozialistischen Regimes in Bulgarien unterstanden alle Nachrichtendienste dem Innenministerium, welches dadurch über enorme Informationsbestände und repressive Instrumente verfügte. Ein solches Monopol wird heute nicht mehr als effektiv angesehen und sogar für gefährlich gehalten. An der heutigen Sicherheitsarchitektur Bulgariens sind mehrere Behörden beteiligt, was die Qualität und Zuverlässigkeit der erhobenen Daten erhöht und die Grundrechte besser garantiert.

1. Die Staatliche Agentur für nationale Sicherheit (SANS)

Diese Behörde wurde 2008 als eine Megastruktur mit weitgehenden Befugnissen gegründet. Die Regierung wollte über eine moderne integrierte Behörde verfügen, und manche nannten sie das „bulgarische FBI“. Tatsächlich war die Gründung der SANS allerdings eine gut gemeinte, jedoch nicht gelungene Idee. Unnötige Verdop-

pelung von Befugnissen mit schon existierenden Diensten, unklare Rechte und Pflichte der Agenten, zu häufige Reformversuche, Personalmangel: Das sind die Hauptprobleme, die die Staatliche Agentur erst mal überwinden muss, um die hohen Erwartungen erfüllen zu können.

Nach Art. 4 des Gesetzes für die Staatliche Agentur für nationale Sicherheit (veröffentlicht im Amtsblatt № 109/20.12.2007)[2], operiert die Agentur in folgenden Hauptaufgabenbereichen: Verteidigung der nationalen Sicherheit, der nationalen Interessen, der Unabhängigkeit und Souveränität des Staates, der territorialen Unversehrtheit, der Grundrechte der Bürger, der demokratischen Funktionsweise der Institutionen und der Verfassungsordnung in Bulgarien. Allein diese Vorschrift zeigt, wie breit und zugleich unklar die Befugnisse der SANS definiert sind.

Nach der Gründung der SANS stellte sich auch die Frage, wie diese Megastruktur ihre Befugnisse in der Strafverfolgung praktisch ausüben wird. Eine entsprechende Änderung in der Strafprozessordnung war erforderlich. Als Resultat wurde eine sehr unklare Rechtsnorm in die bulgarische Strafprozessordnung eingeführt.[3] Art. 194a der bStPO sah den sogenannten Ermittlungsagenten vor; eine neue, für das bulgarische Rechtsystem nicht typische Figur mit unklaren Befugnissen und mangelhaften gesetzlichen Grundlagen. Die gesetzgeberischen Experimente dauerten bis 2015, als diese Rechtsnorm abgeschafft wurde.

Im Bericht der Kommission an das Europäische Parlament und den Rat über die Fortschritte Bulgariens im Rahmen des Kooperations- und Überprüfungsmechanismus für 2014 wird die SANS als eine „hybride" Struktur bezeichnet, in der sich präventiv-operative, nachrichtendienstliche und strafverfolgende Funktionen vermischen, jedoch mit geringer Effizienz und mit großem Risiko für politischen Einfluss.[4] Eine solche Konzentration von Informationssammlung, Repressions- und Ermittlungsbefugnissen kann für die bulgarische Gesellschaft kaum zweckdienlich und nur gefährlich sein.

Die SANS ist ein Sicherheitsdienst, dessen Hauptaufgabe es ist, die nationale Sicherheitspolitik umzusetzen. Grundprinzip der Funktionweise der SANS ist die politische Neutralität.[5] Allerdings ist die Agentur Teil der exekutiven Gewalt und von der Arbeit der Regierung in mancherlei Hinsicht abhängig. Unter diesem Gesichtspunkt lässt sich die Beachtung des Neutralitätsprinzips in Frage stellen. Die immer wieder aufkommenden politischen Skandale, in die der Dienst verwickelt ist, lassen Zweifel an der Neutralität der Behörde entstehen.

So wurde etwa im Juni 2013 eine sehr umstrittene Person zum Direktor der SANS ernannt. Daraufhin begannen sofort Proteste in Sofia und in den anderen Großstädten

---

[2] https://lex.bg/laws/ldoc/2135574489.

[3] Art. 194a der bulgarischen Strafprozessordnung.

[4] https://ec.europa.eu/transparency/regdoc/rep/1/2014/BG/1-2014-36-BG-F1-1.Pdf.

[5] Art. 3, P. 1, 6 des Gesetzes für die SANS.

Bulgariens. Diese Proteste dauerten einige Monate und führten nicht nur zu einem Wechsel des Direktors der Agentur, sondern auch zu einer politischen Krise, in deren Verlauf die Regierung zurücktrat und vorzeitige Parlamentswahlen ausgerufen werden mussten. Im Jahr 2019 entstand ein neuer Riesenskandal und zwar zwischen dem Präsidenten und dem Premierminister: zwei Personen, die sich die Spitze des Staates teilen. Im Kern dieses Skandals stand das illegale Abhören des Präsidenten, das von der Regierung in die Wege geleitet und von der SANS durchgeführt worden sei.

2. Die Staatliche Agentur der Geheimdienste

Die Agentur ist unmittelbar der Regierung unterstellt und operiert meistens außerhalb des Territoriums von Bulgarien. Ihre Hauptaufgabe ist die Verteidigung der äußeren Sicherheit des Staates. Deshalb wird sie mit innenpolitischen Aufgaben nicht beauftragt.[6]

Die Agentur kann spezielle Ermittlungsmaßnahmen sowohl im Inland als auch im Ausland durchführen.[7] Die gesammelten operativ-präventiven und nachrichtendienstlichen Informationen werden zugunsten der nationalen Sicherheit benutzt. Für die Strafverfolgung hat die Agentur keine Befugnisse.

Die Kontrolle über die Tätigkeit der Agentur wird von Premierminister, Präsident und Parlament ausgeübt.

3. Die Dienste „Militärpolizei“ und „Militärinformation“ beim Verteidigungsministerium

Diese Behörden sind unmittelbar dem Verteidigungsminister unterstellt und dementsprechend in der exekutiven Gewalt angesiedelt.

Die Organisation und Funktion der Militärpolizei sind im Gesetz für die Militärpolizei (veröffentlicht im Amtsblatt № 48/24.6.2011)[8] geregelt. Nach Art. 2 dieses Gesetzes hat dieser Dienst sowohl operativ-präventive als auch strafverfolgende Befugnisse.

Kein Gesetz, sondern nur eine Vorschrift der Regierung vom 1.7.2016 reglementiert die Rechtsstellung der Militärinformation.[9] Dieser Dienst sammelt, speichert und bearbeitet operativ-präventive und geheimdienstliche Informationen, die zur Bereitstellung und Unterstützung der bulgarischen Armee, zum Schutz der nationalen Sicherheit und zur Kooperation mit den Partnerdiensten erforderlich sind.

---

[6] Art. 5 des Gesetzes für die Staatliche Agentur der Geheimdienste.

[7] Art. 10 des Gesetzes für die Staatliche Agentur der Geheimdienste.

[8] https://www.lex.bg/laws/ldoc/2135737438.

[9] https://www.lex.bg/bg/laws/ldoc/2136888054.

B. Hauptdirektionen der Nationalpolizei

Das bulgarische Innenministerium schließt vier Hauptdirektionen ein: Hauptdirektion der Nationalpolizei, Hauptdirektion zur Bekämpfung der organisierten Kriminalität, Hauptdirektion der Grenzpolizei und Hauptdirektion des Feuerwehrdienstes[10]. Die ersten drei davon sind für die Verbrechensbekämpfung zuständig.

Das Gesetz für das Innenministerium erlegt der *Hauptdirektion der Nationalpolizei* folgende Aufgaben auf[11]: operative, Bewachung, Strafverfolgung, Information, Kontrolle und Prävention.

Die operative Tätigkeit schliesst einen Komplex von offenen und heimlichen Maßnahmen zur Verbrechensbekämpgung und zum Schutz der nationalen Sicherheit und der öffentlichen Ordnung ein. Das Gesetz für das Innenministerium regelt, welche Strukturen in der Polizei mit diesen Funktionen beauftragt sind.

Zuständig für die Strafverfolgung bei der Polizei sind die sogenannten „Ermittler". Sie sind zwar dem Innenminister unterstellt und Teil der Exekutive, aber agieren unter der Leitung und Aufsicht der Staatsanwaltschaft (die verfassungsrechtlich der richterlichen Gewalt angehört) gemäß den Vorgaben der Strafprozessordnung.

Aus diesem Rechtsrahmen ergibt sich, dass die bulgarische Nationalpolizei gleichzeitig polizeiliche (vorrangig präventive) und strafverfolgende (repressive) Befugnisse hat.

Die Hauptdirektion zur Bekämpfung der organisierten Kriminalität wurde am 13.2.1991 gegründet. Zu diesem Zeitpunkt existierten Dienste mit ähnlichen Funktionen in Großbritannien und in den USA. In ihrer relativ kurzen Geschichte wurde die Direktion mehrmals reformiert und reorganisiert, zwischen 2013 und 2015 funktionierte sie sogar nicht einmal selbstständig, sondern wurde der neu geschaffenen Megastruktur im Bereich der nationalen Sicherheit – der Staatlichen Agentur für nationale Sicherheit, angegliedert. Im 2015 kehrte diese Hauptdirektion aber ins Innenministerium zurück. Daran lässt sich erkennen, dass der bulgarischen Sicherheitsarchitektur eine klare Vision und Stabilität fehlt.

Die Direktion ist Teil der exekutiven Gewalt und dem Innenminister unterstellt. Sie besitzt gleichzeitig operative und strafverfolgende Befugnisse. Dementsprechend sind in der Direktion sowohl operative Polizisten als auch Ermittler angestellt. Sie betreibt Bekämpfung und Verfolgung der organisierten Kriminalität, verbunden mit dem Zoll- und Geldregime, Drogenhandel, Cybercrime, Geld- und Wertzeichenfälschung, Menschenhandel, Kulturgüterhandel, Feuerwaffen und andere gemeingefährliche Mittel, Korruption, Terrorismus, Geldwäsche und illegalem Wetten und

---

[10] Art. 38 des Gesetzes für das Innenministerium.

[11] Art. 39, P. 1 in Verbindung mit Art. 6, P. 1 des Gesetzes für das Innenministerium.

Missbrauch mit europäischen Finanzmittel.[12] Wir können daher sehen, dass sie sehr ähnliche Befugnisse wie die SANS besitzt. Eine Funktionsaufteilung zwischen der Hauptdirektion zur Bekämpfung der organisierten Kriminalität und der Staatlichen Agentur ist gesetzlich nicht geregelt und nur durch Anordnungen des Innenministers reguliert.

Hauptdirektion der Grenzpolizei. Diese spezialisierte Direktion innerhalb des Innenministeriums operiert in der Grenzzone, an den Grenzübergangsstellen, auf den internationalen Flug- und Seehäfen, im Küstenmeer, auf dem Kontinentalschelf, auf der Donau und auf den anderen Grenzflüssen Bulgariens.[13] Sie verfügt über Befugnisse sowohl in der operativen Präventionstätigkeit, als auch in der Strafverfolgung.

C. Die Kommission zur Bekämpfung der Korruption und zur Einziehung des illegal erworbenen Vermögens

Die Kommission ist eine kollegiale staatliche Behörde und besteht aus fünf Mitgliedern, gewählt vom bulgarischen Parlament. Sie wurde 2018 als ein unabhängiger spezialisierter Dienst außerhalb der drei Gewalten gegründet, obwohl seit 2005 Dienste mit ähnlichen Funktionen in Bulgarien existierten. Ihr Hauptziel ist die Bekämpfung der Korruption und Verhinderung der illegalen Bereicherung unter Personen in hohen öffentlichen Ämtern.[14] Die Kommission sammelt operativ-präventive und nachrichtendienstliche Informationen auch mit Hilfe von speziellen Ermittlungsmaßnahmen.[15]

Der Rechtsstatus und die Funktion der Kommission sind in Bulgarien sehr umstritten. Nennenswerte Ergebnisse im Kampf gegen die Korruption hat die Kommission bisher nicht geliefert, wobei man zugestehen muss, dass sie noch nicht sehr lange existiert. Das Gesetz zur Bekämpfung der Korruption und zur Einziehung des illegal erworbenen Vermögens enthält unklare Definitionen von Hauptbegriffen und Maßnahmen, die praktisch schwer umzusetzen sind. Gleichzeitig ist die Kommission ein machtvolles repressiv funktionierendes Organ mit umfangreichen operativen Befugnissen. Meines Erachtens ist sie in dieser Gestalt nicht haltbar und eine Gesetzesreform ist mehr als notwendig.

---

[12] Art. 39 P. 2 des Gesetzes für das Innenministerium.

[13] Art. 39 P. 3 des Gesetzes für das Innenministerium.

[14] Art. 2 des Gesetzes zur Bekämpfung der Korruption und zur Einziehung des illegal erworbenen Vermögens.

[15] Art. 104 P. 3 des Gesetzes zur Bekämpfung der Korruption und zur Einziehung des illegal erworbenen Vermögens.

D. Die Staatsanwaltschaft

Nach der bulgarischen Strafprozessordnung hat im Ermittlungsverfahren unumstritten die Staatsanwaltschaft die führende Rolle. Nur der Staatsanwalt ist berechtigt, eine Klage zu erheben, er hat auch die Entscheidungsgewalt über Gang und Abschluss des Ermittlungsverfahrens. Außerdem ist er gegenüber den Ermittlungsbehörden weisungsbefugt.[16]

Die Staatsanwaltschaft in Bulgarien funktioniert als ein einheitliches und vertikal zentralisiertes System, in dem jeder Staatsanwalt dem oberen unterstellt ist und an dessen Spitze der Generalstaatsanwalt steht.

IV. Nachrichtendienste und spezielle Ermittlungsmaßnahmen

Die Verwendung spezieller heimlicher Ermittlungsmaßnahmen ist eine der wichtigsten Befugnisse der Nachrichtendienste und der Staatsanwaltschaft, mit erheblichen Konsequenzen, die die bulgarische Gesellschaft bereits einige Male zu spüren bekam und deswegen bezüglich dieser Befugnisse ziemlich empfindlich ist.

A. Regelung spezieller Ermittlungsmaßnahmen: historischer Überblick und aktueller Stand

Bis 1993 waren die Anordnung und der Einsatz spezieller Ermittlungsmaßnahmen in Bulgarien gesetzlich nicht geregelt. Diese wurden zunächst durch das Gesetz für die Nationale Polizei (außer Kraft getreten) eingeführt. Ein Jahr später, am 8.4.1994 verabschiedete das Parlament ein besonderes Gesetz für die speziellen Ermittlungsmaßnahmen. Dieses Gesetz bestand aus nur 16 Artikeln und war der erste Versuch des bulgarischen Gesetzgebers, diesem komplizierten und ebenso wichtigen Bereich staatlicher Tätigkeiten einen rechtlichen Rahmen zu geben. Denn auch vor 1993 waren in der Praxis der Polizei und der bulgarischen Geheimdienste die verdeckten Untersuchungsmaßnahmen wie Überwachung, Aufzeichnung von Telekommunikationsinhalten, Observation, Verfolgung u.a. nicht unbekannt. Ihr Einsatz war jedoch nicht durch veröffentlichte Rechtsakte legitimiert, sondern nur in geheimen Anordnungen und Instruktionen der Polizei vorgesehen. Trotz fehlender gesetzlicher Vorschriften ging man damals davon aus, dass die exekutive Gewalt in Bulgarien (Innenministerium und Geheimdienste) zur geheimen Informationssammlung und Informationsspeicherung befugt ist.

---

[16] Art. 46, 196, 197 der Bulgarischen StPO.

In der Strafprozessordnung fehlte ebenfalls eine entsprechende Verrechtlichung. Folglich waren die durch den Einsatz dieser Maßnahmen erzielten Beweisergebnisse im Strafprozess nicht verwendbar.

Die rechtliche Lage ist heute, insbesondere nach dem Eintritt Bulgariens in die EU eine völlig andere. Die Befugnisse der Sicherheitsdienste zur Benutzung der speziellen Ermittlungsmaßnahmen sind nun in mehreren Rechtsakten ausführlich geregelt. Diese lassen sich in drei Hauptgruppen aufteilen:

1. Gesetz für die speziellen Ermittlungsmaßnahmen (GSE)

Das aktuelle Gesetz wurde am 21.10.1997 im Amtsblatt № 95/2017 veröffentlicht. Diesem Gesetz liegt die Grundidee zugrunde, alle speziellen Ermittlungsmaßnahmen in einem Rechtsakt zu erfassen. Zum Umfang des Gesetzes gehören – Definition der Hauptbegriffe, Anordnung und praktischer Einsatz der speziellen Ermittlungsmaßnahmen, Verwertung der Ergebnisse, Löschungspflicht bezüglich der gesammelten Daten, Kontrolle über die Nutzung dieser Maßnahmen. Seit 1997 bis dato gab es fast 40 Änderungen im GSE. Dabei war man immer auf der Suche nach den besten Lösungen in diesem für die ganze Gesellschaft so empfindlichen Gebiet. In den letzten Jahren lässt sich zwar eine deutliche Verbesserung verzeichnen, das Gesetz wird aber von einzelnen Bürgern und Rechtschutzorganisationen immer noch stark kritisiert.

2. Bulgarische Strafprozessordnung (bStPO)

Die aktuelle Fassung der bulgarischen Strafprozessordnung wurde 2005 erlassen. Die Regelung der speziellen Ermittlungsmaßnahmen befindet sich im Vierzehnten Abschnitt, genannt „Ermittlungsmaßnahmen“.[17] Einige Regelungen des GSE werden in der Strafprozessordnung nur wiederholt, andere werden ausführlich neu gefasst. In der bulgarischen StPO liegt natürlich der Schwerpunkt auf dem Einsatz spezieller Ermittlungsmaßnahmen in der Strafverfolgung.

3. Regelung in einzelnen Gesetzen im Bereich der nationalen Sicherheit

Die Ermittlungsbefugnisse der Nachrichtendienste in Bulgarien werden auch in den entsprechenden speziellen Gesetzen geregelt. Diese sind: Gesetz für das Innenministerium (veröffentlicht im Amtsblatt № 53/2014), Gesetz für die staatliche Agentur für nationale Sicherheit (veröffentlicht im Amtsblatt № 109/2007), Gesetz für die staatliche Agentur der Geheimdienste (veröffentlicht im Amtsblatt № 79/2015), Gesetz zur Bekämpfung der Korruption und zur Einziehung des illegal erworbenen Vermögens (veröffentlicht im Amtsblatt № 7/2018).

---

[17] Art. 172–177 der bulgarischen StPO.

B. Einsatzbereiche spezieller Ermittlungsmaßnahmen

Nach der derzeitigen bulgarischen Gesetzgebung können die speziellen Maßnahmen zur Informationssammlung in folgenden Hauptbereichen herangezogen werden:

1. Außerstrafprozessuale operative und ermittelnde Tätigkeit der verschiedenen Dienste der exekutiven Gewalt

Zu Sicherheitszwecken oder zur Aufdeckung von Straftaten sind die Hauptdirektion der Nationalpolizei, die Hauptdirektion zur Bekämpfung der organisierten Kriminalität, die Hauptdirektion der Grenzpolizei, die Direktion „Innere Sicherheit", die Staatliche Agentur für nationale Sicherheit, das Verteidigungsministerium und die Direktion der Geheimdienste befugt, mit Hilfe heimlicher Maßnahmen Informationen zu sammeln, zu speichern und zu verwenden. Wenn diese Informationen auf eine begangene Straftat hinweisen, werden sie an die Staatsanwaltschaft übermittelt, die diese für die Einleitung eines Ermittlungsverfahrens verwenden kann. Sollten die Informationen in der Strafverfolgung nicht benutzt werden können, werden sie archiviert und später nach dem Verstreichen entsprechender Fristen gelöscht. Alle obengenannten staatlichen Behörden sind Teil der exekutiven Gewalt.

2. Als Ermittlungsmaßnahme im Rahmen eines eröffneten Strafverfahrens

Nach der bulgarischen Strafprozessordnung (bStPO) können die speziellen Ermittlungsmaßnahmen zusammen mit den „traditionellen" Mitteln (Vernehmung, Durchsuchung, Beschlagnahme u.a.) zum Sammeln neuer und zur Überprüfung von vorhandenen Beweismitteln eingesetzt werden. Der Einsatz dieser geheimen Maßnahmen zur Erforschung des Sachverhalts unterliegt jedoch strengeren Voraussetzungen:

Diese Maßnahmen sind nicht bei allen Straftaten anwendbar und immer subsidiär. Das ist eine wichtige Garantie gegen unnötige Eingriffe ins Privatleben der Bürger. Außerdem dürfen die Anklage der Staatsanwaltschaft und das Urteil des Gerichts nicht ausschließlich unter Berufung auf Informationen, die mit Hilfe spezieller Ermittlungsmaßnahmen erlangt wurden, begründet werden.[18] Der Grund für ein solches Beweiswürdigungsverbot liegt nicht nur in der Gefahr eventueller Manipulationen. Der Gesetzgeber trägt auch der Tatsache Rechnung, dass die geheimen Maßnahmen verschiedene Grundrechte erheblich einschränken und nie zum Hauptmittel zur Erforschung des Sachverhalts werden sollen.

---

[18] Art. 177 der bStPO.

3. Zum Schutz des Lebens, der Gesundheit und des Eigentums von Personen

Das ist ein besonderer Anwendungsfall der speziellen Ermittlungsmaßnahmen, der eher von sekundärer Bedeutung ist. Er kann sowohl außerhalb als auch innerhalb der Strafverfolgung gegeben sein.[19] Die wohl wichtigste Voraussetzung für den Einsatz ist die ausdrückliche und schriftliche Zustimmung der betroffenen Person. Daraus folgt, dass die speziellen Ermittlungsmaßnahmen auch zur Prävention und zum Schutz von persönlichen Rechtsgütern dienen können.

4. Zum Schutz von Objekten, die mit der nationalen Sicherheit verbunden sind

Zu diesem Zwecke wird von den Behörden des Innenministeriums, des Verteidigungsministeriums, der Staatlichen Agentur für nationale Sicherheit und der Staatlichen Agentur der Geheimdienste auf spezielle Ermittlungsmethoden zurückgegriffen. Die operativ-präventiven und nachrichtendienstlichen Informationen werden zu Sicherheitszwecken gesammelt und gespeichert.

5. Zur Sicherheitsüberprüfung durch die Staatliche Kommission für Informationssicherheit

Nach dem Gesetz zum Schutz klassifizierter Informationen[20] können die speziellen Ermittlungsmaßnahmen zur Sicherheitsüberprüfung von Personen benutzt werden. In solchen Fällen kommt der Einsatz immer nach dem Antrag des Bewerbers, für den das Vorliegen eines bestimmten Sicherheitsniveaus erforderlich ist. Das ist ein Beispiel für die Anwendung der speziellen Ermittlungsmaßnahmen ohne Bezug zur Strafverfolgung.

V. Statistische Daten über die Benutzung spezieller Ermittlungsmaßnahmen und die Arbeit der Nachrichtendienste in Bulgarien

Das Nationale Büro zur Kontrolle der speziellen Ermittlungsmaßnahmen ist ein kollegialer staatlicher Dienst, gegründet im Jahr 2013, der aus fünf Mitgliedern und einer spezialisierten Administration besteht. Die Befugnisse des Büros dienen dazu, die Hauptvorgänge in Verbindung mit den speziellen Ermittlungsmaßnahmen zu

---

[19] Art. 12 P. 2 des Gesetzes für die speziellen Ermittlungsmaßnahmen, Art. 123 P. 7 der bStPO.

[20] Veröffentlicht im Amtsblatt № 45/2002.

kontrollieren: Anwendung, Einsatz, Datenspeicherung und Datenlöschung. Außerdem ist das Büro mit dem Schutz der Grundrechte vor gesetzwidriger Nutzung der speziellen Ermittlungsmaßnahmen beauftragt.[21]

Bis zum 31. Mai jedes Jahres muss das Büro dem Parlament einen Bericht vorlegen. Aus dem Jahresbericht lassen sich sehr wichtige und repräsentative Informationen über die Arbeit der Nachrichtendienste und der Staatsanwaltschaft in Bulgarien entnehmen. Nachfolgend werden wir einen kurzen Überblick der Daten des letzten Berichts (von 2019) geben.[22]

Jahr	Anzahl der eingesetzten Ermittlungsmaßnahmen
2010	5763
2011	8184
2012	5902
2013	4452
2014	4202
2015	2638
2016	2749
2017	2748
2018	3046

Tabelle 1. Einsatz von speziellen Ermittlungsmaßnahmen zwischen 2010 und 2018

Aus diesen Daten können wir folgende Schlüsse ziehen: in Bulgarien ist seit 2011 ein konstanter Trend zur Reduzierung der Anzahl der praktisch eingesetzten speziellen Ermittlungsmaßnahmen erkennbar. Nach 2015 beobachten wir eine relative Stabilisierung. Die Ursachen dafür sind laut Jahresbericht: verstärkte Kontrolle der zweckmäßigen Nutzung der speziellen Ermittlungsmaßnahmen im Rahmen der anordnenden Behörden, eine verbesserte Gerichtsprozedur beim Erlaß der Erlaubnisse und die Arbeit des Nationalen Büros und der anderen staatlichen Diensten. 2018 ist wieder eine Erhöhung der Anzahl der eingesetzten Maßnahmen erkennbar, ein Resultat der Aktivierung der staatlichen Behörden zur Bekämpfung von Korruption und organisierter Kriminalität.

---

[21] Art. 34b–34v des Gesetzes für die speziellen Ermittlungsmaßnahmen

[22] https://www.nbksrs.bg/images/doc/Doc3.pdf

Anordnende Behörde	2016	2017	2018
Innenministerium	56,22%	56,50%	60,78%
SANS	10,08%	6,41%	4,82%
Staatsanwaltschaft	33,39%	36,94%	34,27%
Verteidigungsministerium	0,32%	0,15%	0,13%
Direktion der Geheimdienste	0,00%	0,00%	0,00%

Tabelle 2. Systematisierung der anordnenden Behörde

Sehr wichtige Informationen über die Tätigkeit der Dienste im Bereich der nationalen Sicherheit und der Verbrechensbekämpfung ergeben sich aus Tabelle 2. Die Exekutivorgane (Innenministerium und SANS) greifen am häufigsten auf spezielle Ermittlungsmaßnahmen zurück. Wie schon oben erwähnt, ist im Rahmen eines eröffneten Strafverfahrens ausschließlich die Staatsanwaltschaft für die Nutzung der speziellen Ermittlungsmaßnahmen zuständig. Dementsprechend ist die Anzahl der Anforderungen durch die Staatsanwaltschaft auch relativ hoch und betrifft ungefähr 1/3 der Fälle.

Die Aktivität der Staatlichen Agentur für nationale Sicherheit hinsichtlich der Erhebung nachrichtendienstlicher Informationen reduziert sich ständig (von 10 % im Jahr 2016 auf weniger als 5 % im Jahr 2018). Die Ursachen dafür sind vielfältig. Wir dürfen auch nicht vergessen, dass sich die Hauptdirektion zur Bekämpfung der organisierten Kriminalität zwischen 2013 und 2015 in der SANS befand und danach wieder in das System des Innenministeriums zurückgekehrt ist. Diese Hauptdirektion ist einer der Hauptnutzer spezieller Ermittlungsmaßnahmen.[23]

VI. Interaktion zwischen Nachrichtendiensten und Strafverfolgungsbehörden

Wie schon oben erwähnt, hat sich das System der Nachrichtendienste in Bulgarien seit 1989 sehr dynamisch entwickelt. In den letzten Jahren wurden stets neue Strukturen eingerichtet oder die Befugnisse der existierenden Behörden grundsätzlich reorganisiert, und der Sicherheitsapparat des Staates ist im Ergebnis zu kompliziert geworden. Eine einheitliche staatliche Strategie in Bezug auf die nationale Sicherheit ist kaum zu beobachten, und die Prozesse erfolgen eher konzeptlos und chaotisch.

Zu Beginn der neunziger Jahre war Bulgarien ein nicht reformierter post-sozialistischer Staat, der in seiner künftigen Sicherheitspolitik zwei mögliche Lösungen vor sich hatte – Revolution oder Evolution. Die „revolutionäre“ Lösung hätte die völlige

[23] Siehe oben, III.B.

Auflösung der alten Dienste auf allen Ebenen und die Errichtung eines völlig neuen Sicherheitssystem bedeutet. Das war zum Beispiel der Fall in Polen und in den baltischen Ländern. In Bulgarien wurde der Weg der „Evolution" gewählt. Das heißt, dass nur die Strafverfolgungsbehörde abgeschafft und neu errichtet wurde, wohingegen im Rest des Sicherheitsapparates partielle Reformen durchgeführt wurden. Der wichtigste Vorteil bei dieser Lösung ist, dass große soziale, politische und ökonomische Krisen vermieden werden konnten. Der Nachteil ist aber, dass ein neues System mit vornehmlich altem Personal und technischer Ausrüstung eingerichtet worden ist, sodass man mit den alten Arbeitsmethoden, Instrumenten, Maßnahmen, Kontakten und Abhängigkeiten nicht hat brechen können. Es lässt also gut argumentieren, dass der Einfluss der alten Sicherheitsdienste in Bulgarien noch heute spürbar ist.

Im Ergebnis muss also festgestellt werden, dass in Bulgarien heute keine funktionale und organisatorische Trennung zwischen Nachrichtendiensten und Strafverfolgung existiert. Fast alle Sicherheitsdienste des Staates sind sowohl operativ und präventiv als auch repressiv tätig.

Traditionell ist in Bulgarien das Innenministerium ein großes Machtzentrum. Dessen Mitwirkung an der Strafverfolgung ist auch sehr wichtig, weil die dort angestellten Ermittler bei der Verfolgung von über 80 % aller Straftaten zuständig sind.

Die Idee des Trennungsgebotes ist in Bulgarien praktisch unbekannt; das beste Beispiel dafür ist die SANS. Der Dienst wurde 2008 eingerichtet,[24] und zwar unmittelbar nach dem Eintritt Bulgariens in die EU. Die neue Agentur bekam sofort ein breites Spektrum von Befugnissen ohne Bedenken, dass eine solche Machtkonzentration Nachteile hat und sogar gefährlich werden kann.

Die Nachrichtendienste in Bulgarien funktionieren natürlich nicht isoliert, sie sind Teile eines großen Systems und müssen untereinander interagieren. In den speziellen Gesetzen wird zwar das Prinzip der ständigen Kooperation proklamiert, aber wie das eigentlich praktisch stattfindet, ist unklar. Zwischen den einzelnen Behörden existieren Regelungen, die nur amtlichen Zwecken dienen und oft klassifiziert sind. Als Resultat erfolgt ein mächtiger Informationsaustausch, der in keiner Weise zu kontrollieren ist. Es ist ganz klar, dass die Tätigkeit der Nachrichtendienste nicht öffentlich ablaufen kann und die fehlende Kontrolle den Weg zum Missbrauch ebnet.

Seit einigen Jahren können einzelne Bürger, Medien und Rechtsschutzorganisationen mit Hilfe des Gesetzes über den Zugang zu öffentlichen Informationen[25] Kenntnisse von staatlich gespeicherten Informationen erhalten. Diese sind aber leider sehr sporadisch und können das Gesamtbild der Nachrichtendienste nicht nachzeichnen. Das Informationsdefizit und die fehlende Kontrolle sind direkt mit der Frage des

---

[24] Siehe oben, III.A.1.

[25] https://lex.bg/laws/ldoc/2134929408.

Schutzes der Grundrechte der Bürger verbunden. Offensichtlich muss das bulgarische Sicherheitssystem in dieser Richtung wesentlich verbessert werden.

Im Strafverfahren ist die führende Rolle der Staatsanwaltschaft in Bulgarien unumstritten. Die Verfassung, das Gesetz für die richterliche Gewalt und die Strafprozessordnung definieren klar und deutlich die Befugnisse der Staatsanwaltschaft als einziges Staatsorgan, das berechtigt ist, eine Anklage zu erheben und eine Anklageschrift vor Gericht zu stellen. Alle Behörden, die laut der bulgarischen Gesetzgebung eine Ermittlungsfunktion ausüben, operieren unter der Leitung und Aufsicht der Staatsanwaltschaft.

Das gesamte Beweismaterial, das im Strafverfahren gesammelt wird, wird an die Staatsanwaltschaft weitergegeben und danach hat diese die Entscheidungsgewalt über den Gang und den Abschluss des Ermittlungsverfahrens.

VII. Ausblick

Die Nachrichtendienste haben in Bulgarien einen sehr großen Einfluss auf allen Ebenen des gesellschaftlichen und politischen Lebens, obwohl der größte Teil ihrer Tätigkeit nicht öffentlich erfolgt. Das war so bereits in der sozialistischen Periode des Staates (1944–1989), als das mächtige Komitee für Staatssicherheit operierte. Das Komitee bestand aus sechs Hauptdiensten – Auslandsspionage, Spionageabwehr, Militärspionage, Wissenschaft und Technik, Sicherheit und Bewachung, Bekämpfung der ideologischen Diversion und staatsgefährdender Akte. Letzterer, die sogenannte „sechste Sektion", war die meistgefürchtete politische Polizei, die über tausende Agenten und eine riesige Datenbank verfügte. Leider wurde ein großer Teil des Archivs der sechsten Sektion in den neunziger Jahren heimlich vernichtet, deswegen werden wir nie die ganze Wahrheit erfahren.

Natürlich haben nach 1989 und besonders nach dem Eintritt Bulgariens in die NATO (2004) und in die EU (2007) die Geheimdienste völlig neue Ziele und Aufgaben erhalten. Neue und sehr wichtige Herausforderungen sind die moderne Kriminalität (Terrorismus, Cybercrime, Menschenhandel, organisiertes Verbrechen u.a.) und die heftigen Migrationsprozesse. Die bulgarischen Nachrichtendienste arbeiten nicht nur selbstständig, sondern in Kooperation mit den Diensten der Europäischen Staaten und der USA.

Die Gesetzgebung Bulgariens auf dem Gebiet der Nachrichtendienste hat sich stark verbessert. In den neunziger Jahren war die Regelung in diesem so wichtigen Bereich mehr als mangelhaft. Es gab weder Garantien noch Mechanismen zum Schutz der Grundrechte und des Privatlebens der Bürger. Mit dem Erlass des aktuellen Gesetzes für die speziellen Ermittlungsmaßnahmen (1997) und mit dessen Harmonisierung mit der Strafprozessordnung und mit den anderen speziellen Gesetzen wurde große Fortschritte gemacht. Es lässt sich also feststellen, dass die bulgarische

Gesetzgebung die Standards der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten erfolgreich rezipiert hat. Mit der systematischen Hilfe des Nationalen Büros zur Kontrolle der speziellen Ermittlungsmaßnahmen wird das positive Recht ständig verbessert.

Die Sicherheit des einzelnen Bürgers ist das Hauptziel der Nachrichtendienste und zugleich Hauptkriterium für die Effektivität des ganzen Systems. In dieser Hinsicht existieren noch wichtige Herausforderungen, den die Nachrichtendienste in Bulgarien in den nächsten Jahren gegenüberstehen: bessere technische und personelle Ausrüstung, Anwendung von modernen operativen Maßnahmen, eine verbesserte Zusammenarbeit mit den Diensten anderer Staaten und natürlich die Einhaltung der Grundrechte.

Literaturverzeichnis

Bahchevanov, Georgi, Das Nationale Sicherheitssystem, Sofia, 2007.

Chinova, Margarita, Die Voruntersuchung laut der Strafprozessordnung, Sofia, 2013.

Chinova, Margarita, Benutzung der Daten, bekommen mit Hilfe spezieller ermittlungsmaßnahmen als Beweis im Strafprozess, Modernes Recht, 4-1997.

Chinova, Margarita, Strafprozessualler Zwang und Unversehrtheit der Person, Sofia, 1998.

Grozev, Penjo, Die speziellen Ermittlungsmaßnahmen, gesetzwidrige Anordnung und Einsatz, Sofia, 2017.

Raschkov, Bojko, Die speziellen Ermittlungsmaßnahmen, Sofia, 2010.

Kazakov, Konstantin, Steuerung des Systems für Nationale Sicherheit, Sofia, 2016.

Verbrechensbekämpfung durch Nachrichtendienste in Griechenland

Maria Ntamadaki[1]

[1] Für konstruktive Anmerkungen danke ich Herrn Dr. Mehmet Arslan und Herrn Marc Schmid sehr herzlich.

Einführung

Die Nachrichtendienste in Griechenland stellen für die Öffentlichkeit und die Jurisprudenz eine Black Box dar. Es existieren kaum wissenschaftliche Abhandlungen, die ihre Tätigkeit unter die Lupe nehmen. Fälle, mit denen sich die Rechtsprechung beschäftigt, sind selten. Lediglich in der Presse wird oft über Aufdeckungsfälle berichtet. So war der sog. Vodafone-Skandal ein Fall, bei dem die Telekommunikation einer großen Anzahl von Politikern, einschließlich des Premierministers überwacht wurde und zwar über einen mehrmonatigen Zeitraum in den Jahren 2004 bis 2005, was in der Öffentlichkeit viel Aufsehen erregte. Auch wurde über den Fall einer Entführung von Personen pakistanischer Staatsangehörigkeit im Jahr 2005 durch Agenten des Nationalen Informationsdienstes (EYP) berichtet. Das Ermittlungsverfahren wegen dieser Entführung wurde aufgrund fehlender Beweise eingestellt. In dem Beschluss wurde als Hintergrund des ungeklärten Sachverhalts ein Konflikt innerhalb der pakistanischen Gemeinde Griechenlands angegeben.

Im Vergleich zum EYP ist die Hellenic Financial Intelligence Unit (Hellenic FIU) eher ein junger Dienst. Dass in der Presse kaum Berichte darüber zu finden sind, überrascht deswegen wenig. Auch das Interesse der Öffentlichkeit hinsichtlich der Tätigkeit der nachrichtendienstlichen Direktion der Hellenischen Polizei (DiDAP) kann man als „sparsam" bezeichnen. Dabei stellen viele Praktiken der Strafverfolgungsbehörden im Rahmen der Prävention und der Aufklärung von Verbrechen die rechtsstaatlichen Grenzen des Strafrechtssystems auf die Probe. Hierzu gehören nicht zuletzt die sog. präventiven Festnahmen[2], anonyme Zeugen, Telekommunikationsüberwachung durch die Unterstützung des EYP, pseudonymisierte Nutzerprofile im Internet und Facebook für die Aufdeckung von Pädophilen, usw.[3] Bei näherer Betrachtung des gesetzlichen Rahmens der Nachrichtendienste lässt sich ohne weiteres feststellen, dass es sich um ein komplexes und unübersichtliches Regelwerk handelt. Es besteht aus Normen, die die Aufgaben und Tätigkeiten der Behörden allgemein beschreiben. Die meisten Normen sind Kompetenzverweisungen, interne strukturelle und organisatorische Regelungen sowie Grundlagen für die Einführung neuer Abteilungen mit Koordinationsfunktionen. Gesetzliche Regelungen zu Fragen, wie Nachrichtendienste und Strafverfolgungsbehörden bzw. auch die Nachrichtendienste interagieren sollen, wo die Ermittlungsschwellen liegen und unter welchen Bedingungen ein Informationsaustausch zwischen den Behörden stattfindet, sind nur ansatzweise bzw. kaum vorhanden. Offene Fragen und Auslegungsprobleme lassen

---

[2] Personen werden zu präveniven Zwecken festgenommen, wenn bei der Auswertung der Informationen, die laut der Polizei aus der Überwachung ihrer Aktivität im Internet oder in sozialen Medien gesammelt werden, die Vermutung naheliegt, dass sie im Rahmen einer öffentlichen Versammlung eine Gewalttat insbesondere gegen den Staat oder die demokratische Rechtsordnung begehen könnten. Bedenken hinsichtlich der Verfassungsmäßigkeit einer solchen Maßnahmen angesichts Art. 5 § 4 grGG (Verbot des Freiheitsentzuges durch Verwaltungsmaßnahmen ohne ein Gerichtsurteil) bei *Alivizatos*, NoB 1983, 621, 632.

[3] So bei *Pavlou*, PoinChron 2015, 161.

sich auch nicht anhand der Gesetzesbegründung lösen, denn diese beschränkt sich auf die Darstellung des Regelungsgehalts mit teilweise nur allgemeinen und abstrakten Angaben über die Regelungsratio.

Der vorliegende Beitrag wird sich mit dem Recht der griechischen Nachrichtendienste unter dem besonderen Aspekt der Verbrechensbekämpfung befassen. In einem ersten Teil erfolgt ein kurzer deskriptiver Überblick über die Sicherheitsarchitektur des griechischen Staates (Teil 1.I.). Sodann wird der gesetzliche Rahmen der Nachrichtendienste erläutert (Teil 1. II.A.–D.). Diese Darstellung zeigt auf, wie die Nachrichtendienste für die Verbrechensbekämpfung operationalisiert werden und welche strukturellen und rechtlichen Probleme daraus entstehen (Teil 1. II.E.). Im zweiten Teil wird die Frage aufgeworfen, ob die Struktur und Organisation der Nachrichtendienste den Anforderungen eines gewissen Trennungsgebots entsprechen (Teil 2). Im Anschluss an diese Fragen wird eine Würdigung des gesetzlichen Rahmens de lege lata vorgenommen und Vorschläge für die Grundlagenforschung zum Ziel der Entwicklung eines Nachrichtendienstrechts de lege ferenda in Griechenland unterbreitet.

Teil 1: Grundzüge der Sicherheitsarchitektur

I. Sicherheitsarchitektur: Achse der Topologisierung

Eine Aufgabe des Staates besteht in der Gewährleistung der Sicherheit und Ordnung in einem Staat. Dabei muss der Staat so strukturiert und organisiert werden, dass er diese Aufgabe effektiv erfüllen kann.

Der Begriff „Sicherheit“ wird im griechischen Schrifttum meist im Zusammenhang mit den Begriffen „nationaler und öffentlicher Sicherheit“, „öffentlicher Ordnung“ oder auch der „Polizei“ interpretiert.[4] Vorzugswürdiger erscheint die Erschließung des Begriffs über den der öffentlichen Ordnung. Der Ordnungsbegriff lässt sich besser normativ-theoretisch definieren als der Sicherheitsbegriff. Ordnung bezieht sich auf einen Zustand der Normalität und ihre Funktion besteht darin, diese Normalität der menschlichen Beziehung durch ihre Regulierung mittels Normen zu gewährleisten. Sie hat somit eine regulierende und aufrechterhaltende Wirkung hinsichtlich der Bewahrung der Normalität und der Harmonie der zwischenmenschlichen Beziehungen. Die Ordnung im normativen Sinne bedeutet einerseits die Einhaltung der in concreto geltenden und regulierenden Norm aller Art, andererseits die Einhaltung der Summe aller rechtlichen Normen in einem Staat.[5] Diese normative Erfassung des Ordnungsbegriffs impliziert deutlicher die Anforderungen an Legitimität und

---

[4] So der Versuch der Topologisierung bei *Alivizatos*, NoB 1983, 621, 622–623.

[5] Vgl. *Tachos*, öffentliche Ordnung, S. 15–21.

Legitimation der staatlichen Gewaltausübung. Dabei kann die Ordnung je nach dem Bezugspunkt eine innere (innerhalb eines Staates), eine europäische und eine internationale (völkerrechtliche) Ordnung sein.

Zusammenfassend lässt sich konstatieren, dass die öffentliche Ordnung die Normen über die Beziehungen zwischen Bürger und Staat betrifft. Die innere öffentliche Ordnung des griechischen Staates funktioniert als Sicherheit des Staates und der Bürger. Man unterscheidet innere und äußere Sicherheit.[6] Die innere Sicherheit betrifft alle Gefahren innerhalb, die äußere außerhalb des Staatsgebiets.[7]

Das Heer (Militär, Luftwaffe, Kriegsmarine) dient ausschließlich dem Schutz der äußeren nationalen Sicherheit, d.h. dem Schutz gegen solche Gefahren, die außerhalb des Staatsgebiets entstehen und den Staat als solchen in seiner territorialen Integrität und Souveränität bedrohen.[8] Zuständiges Ministerium ist das Ministerium für die Nationale Verteidigung. Das Heer wird von dem sog. Generalstab der Nationalen Verteidigung (Γενικό Επιτελείο Εθνικής Άμυνας, ΓΕΕΘΑ) geführt, der durch das Zwangsgesetz (Αναγκαστικός Νόμος, Α.Ν.) 1431/1950 gegründet und durch das Gesetz (G.) 2292/1995 reguliert ist. Der Generalstab ist unter anderem auch für die Organisation eines Systems für die Verwaltung von militärischen Informationen zuständig, Art. 11 § 8 lit. ε 2292/1995 (geändert durch Art. 1 § 18 G. 3883/2010). Darauf wird im Rahmen dieses Beitrags nicht eingegangen.

In Griechenland ist das Ministerium für den Bürgerschutz[9] für die innere Sicherheit und öffentliche Ordnung zuständig. Diesem werden drei Behörden zugeordnet, die sich mit der inneren Sicherheit und der öffentlichen Ordnung befassen: die Hellenische Polizei (Ελληνική Αστυνομία, EL.AS.), die Feuerwehr (Πυροσβεστικό Σώμα, P.S.) und das Generalsekretariat für den Zivilschutz (Γενική Γραμματεία Πολιτικής Προστασίας, G.G.P.P.). Die Hellenische Küstenwache (Λιμενικό Σώμα, Λ.Σ.) ist dem Ministerium für Schifffahrt und Inselpolitik untergeordnet und befasst sich mit der inneren Sicherheit im Gewässerbereich. Diese Behörden dienen dem Schutz der inneren nationalen Sicherheit, d.h. dem Schutz gegen solche Gefahren, die innerhalb wie auch außerhalb des griechischen Staatsgebietes entstehen, ohne dass sie Gefahren militärischer Art darstellen. Eine dem deutschen Verfassungsschutz vergleichbare Institution existiert in Griechenland nicht.

Als Polizei (Αστυνομία) im allgemeinen Sinne wird die staatliche Institution mit der Aufgabe definiert, das soziale Verhalten der Bürger und die Einhaltung der Rechtsnormen zu überwachen, für die Prävention, Verfolgung und Repression

---

[6] So *Tachos*, öffentliche Ordnung. S. 22.

[7] Vgl. *Tachos*, öffentliche Ordnung, S. 22–23.

[8] Vgl. *Tachos*, öffentliche Ordnung, S. 22. Das Heer wird in zahlreichen Rechtsnormen des grGG erwähnt, z.B. Art. 4 § 6, 45, 29 § 3 grGG.

[9] Ehemaliges Ministerium für die öffentliche Ordung und zum Schutz der Bürger. Das Ministerium wurde zum Ministerium für den Bürgerschutz mit dem Art. 1 PVO 86/2018 (ΦΕΚ A/159/29.8.2018, S. 9849) umbenannt.

krimineller Handlungen tätig zu werden und dadurch ein friedliches Zusammenleben sowie den Schutz der Menschenrechte zu gewährleisten.[10] Es wird zwischen einer Kriminalpolizei (δικαστική αστυνομία) und einer Verwaltungspolizei (διοικητική αστυνομία) unterschieden. Die Kriminalpolizei befasst sich mit der Strafverfolgung, namentlich der Ermittlung und Aufklärung von Straftaten sowie Vorbereitung des Strafprozesses. Als Strafverfolgungsbehörde hat sie einen justiziellen Charakter und wird grundsätzlich repressiv tätig. Die Verwaltungspolizei ist dagegen grundsätzlich präventiv tätig und ihre Aufgabe besteht in der Gewährleistung der öffentlichen Ordnung und des Friedens.[11]

Der Nationale Informationsdienst (Εθνική Υπηρεσία Πληροφοριών, EYP) war bis Juli 2019 als vierte Sicherheitsbehörde auch dem Ministerium für Bürgerschutz untergeordnet. Ab August 2019 wurde der EYP aus dem Zuständigkeitsbereich dieses Ministeriums ausgegliedert und direkt einer neugegründeten eigenständigen öffentlichen „Stabsstelle", dem sog. „Regierungspräsidium (Προεδρία της Κυβέρνησης)" untergeordnet. Dieses Präsidium wird direkt durch den Premierminister geführt, Art. 21 § 4 G. 4622/2019.[12] Bei dem EYP handelt es sich um einen einheitlichen Inlands- wie auch Auslandsdienst, der sich sowohl mit der inneren wie auch mit der äußeren Sicherheit befasst. Aus diesem Grund ist die Einordnung des Dienstes in der nationalen Sicherheitsarchitektur nicht unproblematisch: Bis zum Jahr 1986 war der EYP dem Premierminister zugeordnet und später dem Ministerium für die öffentliche Ordnung bzw. dem Ministerium für Bürgerschutz.[13]

Im Allgemeinen ist zu bemerken, dass eine Abgrenzung zwischen Justiz- und Verwaltungspolizei in Griechenland zwar funktional vorhanden, jedoch meist unklar ist: Denn oft werden polizeiliche Befugnisse den Verwaltungsorganen eingeräumt und diese können sowohl justiziell bzw. repressiv wie auch administrativ und präventiv tätig werden.[14]

---

[10] So *Papaioannou*, Polizeigewalt, S. 4.

[11] Vgl. *Dimopoulos*, Polizeirecht, S. 40–41; *Papaioannou*, Polizeigewalt, S. 4–5; *Tachos*, öffentliche Ordnung, S. 58 f.

[12] ΦΕΚ/A/133/07.08.2019.

[13] Vgl. *Apostolidis*, EYP, S. 10, 12.

[14] So werden exemplarisch Beamte des öffentlichen Dienstes, etwa in der Zoll- oder Finanzverwaltung Vernehmungs- und Untersuchungsbefugnisse laut der griechischen Strafprozessordnung eingeräumt, s. ausführlich *Tachos*, öffentliche Ordnung, S. 61–63. Auch *Androulakis*, Grundbegriffe, S. 267 Rn. 412; *Papaioannou*, Polizeigewalt, S. 6. Auch polizeilichen Ermittlungsbefugnisse werden der Feuerwehr hinsichtlich der Aufklärung und Verfolgung von Brand- und Waldbrandstiftungsdelikten gem. PVO 3/2000 (ΦΕΚ/A/13.1.2000) und der Hellenischen Küstenwache hinsichtlich der Kriminalität im Gewässerbereich gem. Art. 3 des G. 4150/2013 (ΦΕΚ/A/102/29.4.2013) eingeräumt.

II. Die Nachrichtendienste

In Griechenland existieren drei Behörden, die als Nachrichtendienste zu qualifizieren sind, weil ihre Hauptaufgabe in der Informationsverarbeitung besteht. Diese umfasst drei Stadien: In der Sammlung von unverarbeiteten Informationen (raw intelligence), der Verarbeitung per se und der Übermittlung. Zusätzlich können die Informationsdienste auch Beratung und Anleitung für die Art der Informationen sowie die Bewertung der Qualität und der Wichtigkeit von Informationen leisten.[15]

A. Nationaler Informationsdienst (EYP)

1. Gesetzlicher Rahmen

Dem derzeitigen nationalen Informationsdienst (im Folgenden: EYP) ging der „Zentrale Informationsdienst (Κεντρική Υπηρεσία Πληροφοριών, KYP)" voraus, der im Jahr 1953 durch die Gesetzliche Verordnung Nr. 2421/1953[16] gegründet worden war. Organisiert wurde der KYP nach militärischer Struktur mit Unterstützung und nach dem Vorbild der Central Intelligence Agency (CIA).[17] Er war direkt dem Regierungspräsidenten untergeordnet und seine Mission bestand in der Gewährleistung der nationalen Sicherheit, der Sicherheit des Heers und der Antistaatsspionage, also nur in der äußeren nationalen Sicherheit.

Mit dem Art. 1 des G. 1645/1986[18] wurde der KYP zum „Nationalen Informationsdienst (Εθνική Υπηρεσία Πληροφοριών, EYP)" umbenannt. Schon diese Namensänderung war ein Zeichen des Versuchs der Abkopplung des Dienstes von seiner dunklen Vergangenheit,[19] seiner Entmilitarisierung und Demokratisierung. Der EYP wird durch das G. 3649/2008[20] geregelt. Details über die Organisation von EYP sieht die Präsidialverordnung (PVO) 1/2017[21] vor. Für den EYP gilt auch eine interne Verordnung. Diese normiert noch ausführlicher seine Organisation, Personal-

---

15 Vgl. *Apostolidis*, EYP, S. 13 – 17.

16 ΦΕΚ/A/126/9.5.1953.

17 Vgl. *Tachos*, öffentliche Ordnung, S. 132.

18 ΦΕΚ/A/132/26.8.1986.

19 Der ehemalige Name KYP wurde mit der dunklesten Seite der neugriechischen Geschichte assoziiert. Sowohl in den Zeiten des griechischen Bürgerkrieges ab 1944 wie auch am Höhepunkt der Zeiten der militärischen Diktatur zwischen April 1967 und Juli 1974 wurde der KYP zur massiven Überwachung, Gewaltanwendung, Verfolgung, Vertreibung und Vernichtung von Oppositionellen und Bekämpfern der Diktatur sowie Anhängern von kommunistischer Ideologie instrumentalisiert. Vgl. u.a. *Tachos*, öffentliche Ordnung, S. 133.

20 ΦΕΚ 39 / 545/3.3.2008. Das G. 1645/1986 wurde mit dem Art. 27 des G. 3649/2008 außer Kraft gesetzt.

21 ΦΕΚ/A/2/17.1.2017. Diese PVO setzte außer Kraft die bisher geltende PVO 126/2009 (ΦΕΚ/A/173/7.9.2009).

angelegenheiten sowie die besonderen und speziellen Aufgaben und Befugnisse der Direktion des EYP. Diese interne Verordnung wird gem. Art. 12 des G. 3649/2008 im staatlichen Gesetzesblatt nicht veröffentlicht und ist als „Staatsgeheimnis" eingestuft.

2. Aufgaben des EYP

Gem. Art. 2 § 1 des G. 3649/2008 besteht die Aufgabe des EYP in der Sammlung, Verarbeitung und Übermittlung von Informationen an die zuständigen Behörden, und zwar:

a) zum Schutz und zur Förderung der politischen, ökonomischen, militärischen und allgemeinen nationalen Interessen des Staates,
b) zur Prävention und Bekämpfung von Aktivitäten, die eine Bedrohung für die demokratische Staatsform, die Grundfreiheiten des Menschen, die territoriale Integrität und die nationale Sicherheit und die Ressourcen des Staates darstellen und
c) zur Prävention und Bekämpfung von Aktivitäten terroristischer Organisationen und anderer Gruppen der organisierten Kriminalität.

Subsidiär wird in Art. 2 § 2 G. 3649/2008 die Aufgabe und die Rolle des EYP in Krisenfällen normiert. Im Kriegsfall oder im Falle einer Mobilmachung oder einer unmittelbaren Bedrohung für die nationale Sicherheit wird der EYP dem obersten Offizier des Heers, dem sog. Generalstab der Nationalen Verteidigung (Γενικό Επιτελείο Εθνικής Άμυνας, ΓΕΕΘΑ), untergeordnet, der dann die Verteidigung des Staates koordiniert. Im Falle gewaltsamer Aktivitäten mit dem Ziel der Auflösung der demokratischen Staatsform wird der EYP zum zentralen Dienst der Informationenverwaltung des Staates berufen.[22]

3. Modus Operandi des EYP

Der Modus Operandi des EYP wird in Art. 5 G. 3649/2008 beschrieben. Es besteht in der Sammlung von Informationen durch entweder technische Mittel (sog. Sigint: signalerfassende Aufklärung) oder durch menschliche Quellen (Humint, z.B. durch Agenten). Die Informationsbeschaffung erfolgt durch Überwachung und Aufzeichnung der Aktivität von Personen mit optischen und akustischen technischen Mitteln und durch verdeckte Ermittlungen. EYP-Agenten dürfen unter Verdeckung ihrer

[22] Die Berufung erfolgt durch einen Beschluss des sog. Regierungsrates über Außenverhältnisse und Verteidigung (Κυβερνητικό Συμβούλιο Εξωτερικών και Άμυνας, KYSEA), dessen Direktor der Premierminister ist.

Identität, Eigenschaft, ihrer beruflichen Tätigkeit vereinzelt oder kollektiv agieren, wie dies in der internen Verordnung der EYP normiert ist.[23]

Weitere Details über den Modus Operandi des EYP sind dem Gesetz nicht zu entnehmen. Ob z.B. der EYP von unmittelbarem Zwang etwa durch den Einsatz von Waffen Gebrauch machen oder ob und ggf. welche Zwangsmaßnahmen er in Einzelfällen heranziehen darf, ist im Gesetz nicht geregelt. Bei näherem Hinsehen offenbart sich, dass die Frage, ob der EYP eine Art polizeiliche Exekutivgewalt ausübt, an sich dem Grundsatz der Geheimhaltung unterliegt.[24] Denn es ist nicht auszuschließen, dass die interne Verordnung explizite und ausführliche Normen auch hinsichtlich womöglich existierender Exekutivbefugnisse des EYP enthalten, diese sind aber als Geheimnis eingestuft und der Öffentlichkeit nicht zugänglich.

Gem. Art. 4 Nr. 4 G 3649/2008 „kümmert sich" (so die wörtliche Übersetzung von „μεριμνά" im Wortlaut) der EYP um die Bekämpfung der Spionageaktivitäten gegen den Staat. Diese Norm ist unbestimmt. Der Wortlaut gibt keine Informationen darüber worin dieses „Sich-Kümmern" besteht und welche Bedingungen für seine rechtmäßige Ausübung gelten. Der Wortlaut spricht nicht zwingend für eine Beschränkung auf die bloße Informationsbeschaffung über Spionage-Aktivitäten. Denn Sich-Kümmern kann auch die aktive Bekämpfung der Spionage bedeuten. Deswegen ist nicht auszuschließen, dass der EYP auch aktive Maßnahmen gegen Spionage vornimmt.[25]

An dieser Stelle ist anzumerken, dass Art. 5 § 4 G. 3649/2008 mindestens Teilen des Personals des EYP das Recht einräumt, Waffen zu besitzen und mit sich zu tragen. Laut dem Wortlaut darf das Personal des EYP diese nur zum eigenen Schutz und zum Schutz der Anlagen besitzen, tragen und nutzen.

Außerdem ist gem. Art. 4 § 8 G. 3649/2008 der EYP die Nationale Behörde für die Bekämpfung elektronischer Angriffe (Nationaler CERT). Seine Funktion besteht in der Prävention sowie der Prävention und aktiven Bekämpfung elektronischer Angriffe auf Kommunikationsnetzwerke, Anlagen zur Informationsspeicherung und Informationssysteme, vor allem im öffentlichen staatlichen Bereich und in den kritischen Infrastrukturen des Staates. Als nationaler CERT verfügt er über das erforderliche wissenschaftliche Personal und die notwendige technische Ausstattung, um solche Angriffe abzuwehren, die Bekämpfungsstrategie dafür zu entwickeln sowie Informationen diesbezüglich zu sammeln, zu verarbeiten und weiterzuleiten. Es handelt sich wiederum um eine weit angelegte Gesetzesnorm. Denn Bekämpfung und Prävention meinen wohl nicht nur die Informationsbeschaffung

---

[23] Vgl. auch zum Modus Operandi der Nachrichtendienste, *Apostolidis*, EYP, S. 14–15 (allgemein), S. 20 (EYP); zum sog. Intelligence Cycle s. *Zöllner*, JZ 2007, 763, 766.

[24] Vgl. auch *Papaioannou*, Polizeigewalt, S. 41.

[25] Vgl. auch *Papaioannou*, Polizeigewalt, S. 42; *Tachos*, öffentliche Ordnung, S. 134.

durch die Überwachung der elektronischen Aktivität, sondern auch die Aufklärung und eine aktive Abwehr elektronischer Angriffe.

Über die genaue Vorgehensweise des EYP hinsichtlich der Bekämpfung der Cyberkriminalität gilt eine interne Verordnung, die öffentlich zugänglich ist.[26] Insbesondere gem. Nr. 4.1. der Verordnung sammelt und sichert der EYP als CERT Beweismaterial für elektronische Angriffe und Bedrohungen aus öffentlichen und privaten Organisationen und kritischen Infrastrukturstellen. Gem. Nr. 5 der Verordnung unterstützt der EYP die Informationssystembetreiber, auf einen Bedrohungs- oder Angriffsfall zu reagieren. Als Reaktion des EYP kommen die Analyse und Bewertung, Koordination und entsprechende Maßnahmen in Betracht. Die Analyse betrifft die Frage, ob der Vorfall als ein Fall für die informationstechnische Sicherheit einzustufen ist und welchen Umfang er hat. Die Analyse besteht in der Sammlung, Bewahrung, Dokumentation und Analyse von Daten aus einem Computersystem, das beschädigt bzw. angegriffen worden ist. So werden die Veränderungen in diesem System bestimmt und die Ereignisse rekonstruiert, die zum Angriff geführt haben. Die Lösung des Falles wird beobachtet und alle Fälle von Angriffen und Bedrohungen werden archiviert. Jedoch tragen die Inhaber der jeweiligen Informationssysteme die Verantwortung für den sicheren Betrieb sowie für die jederzeit mögliche Lösung eines Vorfalles in diesen Systemen.

Neben der Informationsbeschaffung hat der EYP auch Beratungs- und Begutachtungsfunktionen sowohl in Friedens- wie auch in Krisenzeiten. Der EYP darf gem. Art. 5 § 2 G. 3649/2008 im Rahmen der Kontrolle einer Person bei ihrem Ein- bzw. Austritt aus dem griechischen Staatsgebiet gem. Art. 5 G. 3386/2005[27] Stellung dazu nehmen, ob ein Ausländer für die nationale Sicherheit gefährlich ist sowie ob die Voraussetzungen über seine Einstufung als „unerwünscht" vorliegen. Dies ist ein weiterer Indikator dafür, dass der EYP Beobachtungsmaßnahmen auch einzelfallbezogen ergreifen darf. Schließlich darf er gem. Art. 4 Nr. 1 G. 3649/2008 Vorschläge über die Prävention und Abwehr von Bedrohungen der nationalen Sicherheit und der demokratischen Staatsform an den zuständigen Minister vorlegen.

4. Ermittlungsschwelle

Das G. 3649/2008 enthält nur Ausführungen über die formalen Voraussetzungen für den Beginn der operativen Tätigkeit des EYP sowie über die gesetzlichen Grenzen seiner Tätigkeit. Ob der EYP auf jeden Anlass oder nur im Falle eines gewissen Verdachtsgrades etwa analog zu dem nach der grStPO im strafrechtlichen Ermittlungsverfahren geltenden Verdachtsgrade tätig wird, ergibt sich aus dem Gesetz

---

[26] Interne Verordnung vom 26.9.2016, Auflage 1.0 (auf Griechisch), abrufbar unter http://www.nis.gr/npimages/docs/displayDoc_gr.pdf [Stand: 20.12.2019].

[27] ΦΕΚ/A/212/23.8.2005 über den Zutritt, Aufenthalt und Integration von Bürgern aus Nicht-EU-Staaten im griechischen Staatsgebiet.

nicht. Dadurch, dass sich keine Begrenzungen aus dem Gesetz ergeben, kann davon ausgegangen werden, dass der EYP sowohl einzelfallabhängig, z.B. im Rahmen seiner Stellungnahme über die Gefährlichkeit eines einreisenden Drittstaatsbürgers, wie auch einzelfallunabhängig tätig wird. Jeder Anlass für die Überprüfung und Verarbeitung einer Information im Bereich seiner Zuständigkeit kann ausreichend sein. Das Gesetz enthält keine Ausführungen über die Anforderungen und den Inhalt eines Anlasses. Beschränkungen hinsichtlich des konkreten Vorgehens des EYP können sich jedoch aus dem Grundgesetz sowie im Fall der technischen Überwachung aus den Verfahrensvoraussetzungen für die Aufhebung von Kommunikationsgeheimnissen gem. den entsprechenden Gesetzen zum Schutz des Kommunikationsgeheimnisses und der Privatsphäre ergeben.[28]

B. Direktion für die Verwaltung und Analyse von Informationen der EL.AS. (DiDAP)

1. Gesetzlicher Rahmen

Die Direktion für die Verwaltung und Analyse von Informationen (Διεύθυνση Διαχείρισης και Ανάλυσης Πληροφοριών, im Folgenden: DiDAP) wurde als selbstständiger zentraler Informationsdienst der Hellenischen Polizei (EL.AS.) nach Art. 22 des G. 4249/2014[29] gegründet. Dieser Artikel und Art. 27 der PVO 178/2014[30] stellen den geltenden gesetzlichen Rahmen über die Organisation und Tätigkeit der DiDAP dar.

2. Aufgaben der DiDAP

Die Aufgabe der DiDAP wird in Art. 22 § 1 G. 4249/2014 festgelegt. Sie besteht zum einen in der Sammlung, Auswertung, Einordnung, Analyse und Vermittlung von Informationen zum Zweck der Bekämpfung der organisierten Kriminalität und des Terrorismus, zum anderen in der Bewahrung, Sicherung und Aktualisierung von speziellen Datenbanken.

3. Modus Operandi der DiDAP

Ihr Modus Operandi wird durch den Art. 27 PVO 178/2014 und die interne Verordnung der Direktion geregelt, die aber der Öffentlichkeit nicht zugänglich ist. Die DiDAP sammelt Informationen sowohl durch selbstständige operative Tätigkeit wie

---

[28] S. unten Teil 2.III.C.1.b).bb).

[29] ΦΕΚ/A/73/24.3.2014. Dem Art. 22 wurde durch Art. 231 § 3 G. 4281/2014 (ΦΕΚ/A/160/8.8.2014) sind zwei neue Absätze Nr. 5 und 6 hinzugefügt.

[30] ΦΕΚ/A/281/31.12.2014.

auch aus allen Abteilungen und Direktionen von EL.AS., den Justizbehörden und anderen Rechtsdurchsetzungsbehörden[31] (vgl. Art. 27 § 2 lit. a PVO 178/2014). Auch sammelt sie Informationen durch die Verwendung von modernen elektronischen und speziellen technischen Systemen (so Art. 24 § 4 lit. a PVO 178/2014). Weitere Details über den Modus Operandi der DiDAP sind den genannten Rechtsnormen nicht zu entnehmen. Die weiteren im Art. 27 PVO 178/2014 beschriebenen Tätigkeiten beziehen sich auf organisatorische Verwaltungsmaßnahmen, die Erstellung von Berichten sowie Erklärungen über den Umgang mit Informationen, z.B. dass die DiDAP die gesammelten Informationen zum Zweck einer Operationsplanung nutzt. Die DiDAP als der Nachrichtendienst der Polizei unterstützt die Polizei und die Strafverfolgungsbehörden grundsätzlich informatorisch, z.B. pflegt sie das Archiv und die Datenbank der EL.AS., oder sie vermittelt Informationen und stellt ihre informationstechnische Ausstattung für die Ermittlungen zur Verfügung, wenn dies notwendig ist.

Bemerkenswert ist, dass der DiDAP in Ausnahmenfällen vollzugspolizeiliche Befugnisse zustehen, wie dies in Art. 22 § 6 G. 4249/2014[32] i.V.m. Art. 6 G. 2713/1999 und Art. 3 G. 2225/1994 geregelt wird. Während einer Voruntersuchung oder im Rahmen von Vorermittlungsverfahren wegen einer der im Gesetz aufgezählten Straftaten (z.B. Staatschutzdelikte, Urkundenstraftaten, Drogenkriminalität, Gewalttaten usw.) darf der Staatsanwalt, der die Aufsicht über die DiDAP ausübt, einen Antrag auf die Aufhebung des Kommunikationsgeheimnisses vor dem Revisionsrat der Staatsanwaltschaft stellen. In besonders eiligen Fällen darf der Staatsanwalt dies auch selbst anordnen. Die Aufhebung des Kommunikationsgeheimnisses ermöglicht die Telekommunikationsüberwachung. Mit dem gleichen Verfahren darf auch die Aufhebung des Bankgeheimnisses angeordnet werden, die dann weitere Maßnahmen, namentlich eine Überwachung der Finanztransaktionen und eine Vermögenssperre, ermöglicht. Auch können weitere optisch-akustische Überwachungsmaßnahmen angeordnet werden. Im Rahmen der Ermittlung einer Steuerstraftat gilt das Steuergeheimnis gegenüber der DiDAP nicht. Informationen, die im Rahmen dieser Maßnahmen gesammelt werden, werden in die Akte aufgenommen und können als Beweismaterial dienen (Art. 5 § 9 S. 2 G. 2225/1995). So können Informationen, die die DiDAP im Rahmen eines Untersuchungsverfahrens gesammelt hatte, in das strafrechtliche Ermittlungsverfahren gelangen.

---

[31] Gem. Art. 27 § 13 lit. a PVO 178/2014 eine Rechtsdurchsetzungsbehörde im Sinne dieses Gesetzes ist jede Behörde mit der Aufgabe von Aufklärung, Prävention und Ermittlung von Straftaten. Dazu zählt der Artikel u.a. auch die EL.AS., die Feuerwehr und die Hellenische Küstenwache.

[32] Eingefügt durch Art. 231 § 3 N. 4281/2014 (ΦΕΚ/A/160/8.8.2014).

4. Ermittlungsschwelle

Wann die DiDAP für die Sammlung der Informationen tätig werden darf, wird im Gesetz nicht allgemein bestimmt. Anhaltspunkte dafür lassen sich jedoch aus den einigen Rechtsnormen entnehmen.

Art. 27 § 13 PVO 178/2014 unterscheidet zwischen der Ermittlung von Straftaten und der Sammlung von Informationen im Sinne des Gesetzes über die DiDAP. Gem. Art. 27 § 13 lit. β PVO 178/2014 betrifft die „Untersuchung von Straftaten" das Verfahrensstadium, nach dem die zuständige Rechtsdurchsetzungsbehörde Maßnahmen für die Feststellung der Begehung einer Straftat, der Umstände dieser Tat sowie der potentiellen Täter ergreifen. Gem. Art. 27 § 13 lit. γ der PVO 178/2014 betrifft die Sammlung der Information dagegen jenes Verfahrensstadium, das noch nicht das „Stadium der Untersuchung für eine Straftat" erreicht hat und in dessen Rahmen die Rechtsdurchsetzungsbehörden die Zuständigkeit haben, Informationen zu sammeln, zu analysieren und zu verarbeiten, damit sie feststellen, ob eine oder mehrere Straftaten begangen worden sind. Das „Stadium der Untersuchung einer Straftat" im strafprozessualen Sinne wird beim Vorliegen von hinreichenden Hinweisen auf die Begehung einer Straftat erreicht (sog. Anfangsverdacht), gem. Art. 43 § 1 S. 2 grStPO.

An dieser Stelle ist zu bemerken, dass im griechischen Strafprozessrecht drei Stadien des Ermittlungsverfahrens vorgesehen sind: Zu unterscheiden ist zwischen einem Untersuchungs- (προκαταρκτική εξέταση), einem Hauptermittlungs- (κύρια ανάκριση) und einem Vorermittlungsverfahren (προανάκριση), je nachdem, ob es sich um ein Verbrechen bzw. schweres Vergehen oder ein milderes Vergehen handelt. Ein Untersuchungsverfahren hat die Prüfung der Voraussetzungen für die Eröffnung eines Ermittlungsverfahrens zum Gegenstand. Dieses ist Voraussetzung für die Eröffnung des Hauptermittlungsverfahrens im Fall eines Verbrechens. Für die Eröffnung des Haupt- bzw. Vorermittlungsverfahrens ist das Vorliegen von hinreichenden Anhaltspunkten für eine Straftat erforderlich (Art. 43 § 1 S. 2 grStPO).[33] Für das Untersuchungsverfahren sieht der Wortlaut des Art. 243 grStPO keine konkrete Ermittlungsschwelle vor. Es ist davon auszugehen, dass jeder Hinweis auf den Verdacht einer Straftat genügt.

Wenn das Stadium der „Sammlung der Informationen" schon vor dem Stadium eines Untersuchungsverfahrens im Sinne des Art. 243 grStPO liegt, bedeutet dies, dass der DiDAP auch in einem sehr weiten Vorfeld tätig wird. Die polizeiliche Informationssammlung darf also bei bloßen Vermutungen oder jedem Anlass unter der genannten Schwelle der hinreichenden Hinweise bzw. des Anfangsverdachts im Sinne der grStPO betrieben werden.

---

[33] Vgl. *Androulakis*, Grundbegriffe, S. 269 Rn. 420.

C. Hellenic Financial Intelligence Unit (Hellenic FIU)

1. Gesetzlicher Rahmen

Die erste institutionelle Form der Financial Intelligence Unit in Griechenland war die Kommission für die Bekämpfung der Geldwäsche und der Terrorismusfinanzierung, die im Jahr 2008 gegründet worden war (Art. 7 des G. 3691/2008[34]). Mit dem G. 3932/2011[35] wurde diese Kommission durch eine unabhängige Behörde mit dem Namen „Behörde für die Bekämpfung der Legalisierung von Einkünften aus krimineller Aktivität und für die Terrorismusfinanzierung sowie für die Kontrolle der Vermögenserklärungen" ersetzt. Mit Art. 47 G. 4557/2018[36] wurde diese Behörde schließlich zur „Behörde für die Bekämpfung der Legalisierung von Einkünften aus Straftaten" umbenannt und umstrukturiert. Diese Behörde wird mit Art. 3 Nr. 22 des G. 4557/2018 als die nationale Financial Intelligence Unit für Griechenland (im Folgenden: Hellenic FIU) bezeichnet.

2. Aufgaben der Hellenic FIU

Die Hellenic FIU sammelt, verwaltet und analysiert Informationen über die Finanz- und Vermögensverhältnisse von Personen. Die Informationssammlung geschieht zur Erfüllung ihrer Aufgabe, die gem. Art. 47 Abs. 1 G. 4557/2018 in Folgendem besteht:

a) Ergreifen und Anwendung von Maßnahmen zur Prävention, Bestimmung und Bekämpfung der Geldwäsche und der Terrorismusfinanzierung;

b) Bestimmung der Personen, die einen Bezug zum Terrorismus haben, sowie Festsetzung und Vollzug von finanziellen Sanktionen gegen diese sowie auch gegen diejenigen Personen, die vom Sicherheitsrat oder den Organen der UNO oder durch Beschlüsse und Verordnungen aus der Europäischen Union bestimmt werden;

c) Prüfung der Vermögenserklärungen von Personen, die gem. G. 3213/2003[37] der steuerrechtlichen Pflicht unterliegen, die Herkunft größerer Geldsummen offenzulegen (sog. Πόθεν έσχες, d.h. „woher man etwas hat").

---

[34] ΦΕΚ/A/166/5.8.2008.

[35] ΦΕΚ/A/49/10.3.2011.

[36] ΦΕΚ/A/139/30.7.2018. Das Gesetz ersetzt das G. 3691/2008 und dient der Umsetzung der Richtlinie 2015/849/EU zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung vom 20.5.2015. Art. 47 G. 4557/2018 entspricht Art. 32 §§ 1, 3 der RL.

[37] ΦΕΚ/A/309/31.12.2003, wie dieses durch das G. 4571/2018 (ΦΕΚ/A/186/30.10.2018), verändert wurde.

3. Modus Operandi der Hellenic FIU

An die Hellenic FIU werden Meldungen über verdächtigte Transaktionen (suspicious transactions reports) und Informationen über kriminelle Tätigkeiten im Bereich des Terrorismus und der Terrorismusfinanzierung weitergeleitet. Die Behörde wird in drei selbstständige Einheiten untergliedert, die unterschiedliche Aufgaben, Personal und Infrastruktur bereithalten, jedoch einem gemeinsamen Präsidenten unterstehen, so Art. 48 § 1 G. 4557/2018.

Die Aufgaben der Einheit A werden in Art. 48 § 2 G. 4557/2018 beschrieben. Sie ist zuständig: für die Sammlung und Verarbeitung von finanzwirtschaftlichen Informationen; für die Beratung der gem. Art. 5 des G. 4557/2018 meldepflichtigen Personen; für die operativen Analysen zum Zweck der Analyse und Verbindung von Fällen, der Bestimmung von kriminellen Netzwerken oder Gruppen oder einzelnen Verdächtigen sowie der Aufklärung der Art ihrer Tätigkeit, wenn Hinweise oder Verdacht auf Geldwäsche oder Terrorismusfinanzierung bestehen; für strategische Analysen, die hilfreich für die Anerkennung und Systematisierung der üblichen Praktiken von Geldwäsche und Terrorismusfinanzierung sind.

Die Aufgaben der Einheit B bestehen gem. Art. 48 § 3 G. 4557/2018 in der Verhängung und dem Vollzug von finanzwirtschaftlichen Sanktionen. Auch sammelt und bewertet sie Informationen über die Begehung einer Straftat der organisierten Kriminalität. Diese Informationen werden durch andere polizeiliche oder staatsanwaltliche Behörden, durch andere internationale Informationsbehörden und FIUs oder in sonstiger Weise an die Behörde übermittelt. Der Präsident und die Einheit B sind auch für die Vermögensperre gegen Personen zuständig, die durch Beschlüsse des Sicherheitsrates oder der Organe der UNO sowie durch Beschlüsse und Verordnungen der Europäischen Union angeordnet werden. Die Einheit B ist weiterhin zuständig für die Identitätsbestimmung und die Vermögensperre von Personen, die in Verbindung mit Terrorismus stehen.

Die dritte Einheit C ist für die Kontrolle der Vermögenserklärung von Personen zuständig, die zur Offenlegung ihrer Vermögensverhältnisse gesetzlich verpflichtet sind, z.B. der Premierminister, Parlamentsabgeordnete, Personen der öffentlichen Verwaltung, Eigentümer und Anteilsinhaber von Medien, die Direktoren von EL.AS., der Hellenischen Küstenwache und Feuerwehr, Richter und Staatsanwälte der höchsten Gerichtsbarkeit etc. Die Funktion der Einheit C besteht gem. Art. 48 § 4 G. 4557/2018 darin, dass sie die zuständige Behörde für die Annahme der Vermögenserklärungen der verpflichteten Personen ist. Sie darf die Vermögenserklärungen der verpflichteten Personen prüfen. Ob die Prüfung geplant und vorangemeldet oder stichprobenartig geschieht, darf sie nach eigenem Ermessen entscheiden. Prüfungsgegenstand ist die Richtigkeit der Angaben in der Vermögenserklärung, die Tatsache der Abgabe der Vermögenserklärung überhaupt sowie die Frage, ob der Erwerb neuer Vermögenswerte und der Zuwachs bereits bestehenden Vermögens anhand der Höhe des Einkommens als angemessen und gerechtfertigt erscheint. Die

Einheit C darf Unterlagen und Informationen von jeder Behörde, Organisation oder Person verlangen, die auch zur Informationsvermittlung verpflichtend sind. Nach Beendigung einer Prüfung entscheidet die Einheit C, ob der Fall archiviert oder an den zuständigen Staatsanwalt übermittelt wird, soweit sich hinreichende Anhaltspunkte für eine Straftat aus der Prüfung ergeben.

Art. 48 § 2 Fall δ) G. 4557/2018 sieht als Befugnis der Behörde vor, in Eilfällen sogar Zwangsmaßnahmen zu ergreifen, wenn ein Verdacht bzw. Hinweis besteht, dass ein Vermögen oder eine Transaktion im Zusammenhang mit Geldwäsche oder Terrorismusfinanzierung steht. Auf Anordnung ihres Präsidenten oder einer entsprechenden Behörde eines EU-Mitgliedstaates darf die Hellenic FIU das Vermögen vorübergehend sperren oder die Transaktion einstellen, bis sich der Verdacht als begründet bzw. schlüssig erweist. Diese Maßnahmen dürfen nur bis zu 15 Werktage dauern. Nach Ablauf der Frist von 15 Tagen entfallen diese Maßnahmen von Rechts wegen, wenn sich der Verdacht nicht bestätigen lässt. Ergibt sich aus dieser Untersuchung jedoch ein hinreichend schlüssiger Verdacht, dann wird die Beschlagnahme des Vermögens der unter Verdacht stehenden Personen vom Präsidenten gem. Art. 42 § 5 des G. 4557/2018 angeordnet. Die Behörde darf nach der Beendigung der Untersuchung darüber entscheiden, ob der Fall archiviert oder mit einem begründeten Bericht an den zuständigen Staatsanwalt übermittelt wird.

Die Hellenic FIU operiert auch im Bereich des Terrorismus gem. Art. 50 des G. 4557/2018. An sie werden Beweise und Informationen jeder Art von den polizeilichen, justiziellen und anderen Behörden übermittelt, die sich im Rahmen eines Ermittlungs- oder Gerichtsverfahrens oder sonstigen Prüfungsverfahrens in Zusammenhang mit Terrorismus ergeben, z.B. Anklagen oder Gerichtsurteile. Die Behörde speichert all diese Informationen und Beweise und führt einen Katalog mit den betroffenen Personen und ihren Daten, die zu genauen Identitätsfeststellungen führen können. Sie informiert alle meldepflichtigen Personen über den Katalog, die dann verpflichtet werden, jede Information über dies betreffenden Personen an die Hellenic FIU weiterzuleiten. Die Hellenic FIU ist sogar befugt das Vermögen dieser Personen im Katalog zu sperren und jegliche Transaktion oder Vermögensverfügung zu verhindern. Sie darf diese Informationen und Daten auch an internationalen FIU und anderen Behörden übermitteln wie auch von diesen Behörden Informationen verlangen. All diese Informationen und Daten sammelt die Hellenic FIU ausschließlich und nur mit dem Ziel der Verhängung von wirtschaftlichen Sanktionen, wie Art. 51 § 5 G. 4557/2018 bestimmt. Auch sammelt die Hellenic FIU Informationen und ergreift Maßnahmen, wie Vermögensperren, Beschlagnahmen, vor Ort durchgeführte Durchsuchungen von Einrichtungen und Personen in Fällen der Terrorismusfinanzierung.

Hinsichtlich der Tätigkeit der Hellenic FIUs bestehen Bedenken in zwei Richtungen. Wird gegen eine Person durch die Hellenic FIU ermittelt, bleibt die verdächtigte Person in Unkenntnis darüber. Dies wird sogar gesetzlich bestimmt. Art. 27 G. 4557/2018 sieht das Verbot für die meldepflichtigen Personen vor, die von der

Meldung betreffenden Person oder Dritten über die Meldung oder die Tatsache in Kenntnis zu setzen, dass sie Informationen an die Hellenic FIU übermittelt haben. Der Verstoß gegen dieses Verbot stellt nicht nur eine disziplinarrechtliche Verletzung, sondern auch eine Straftat dar, die mit Freiheitsstrafe von mindestens drei Monaten zu bestrafen ist. Dies ist einerseits nicht neu. Ermittlungsmaßnahmen durch die Strafverfolgungsbehörden bleiben grundsätzlich auch zunächst geheim. Aber die grStPO sieht Pflichten für die Information und das Gehör der betreffenden Person vor. Eine solche Pflicht wird für die Nachrichtendienste nicht konstituiert. Es kann also vorkommen, dass die Vermögensverhältnisse einer Person überwacht werden, über diese Person Informationen gesammelt werden und diese Person bis zur Übermittlung der Akte an die Staatsanwaltschaft keine Kenntnis davon hat.

Das zweite Problem liegt darin, dass keine Obergrenze für die Dauer der Ermittlungen und der Informationssammlung ausdrücklich gesetzlich bestimmt ist. Im Rahmen der Überwachung durch EYP und DiDAP wird auf die Garantien der G. 2225/1994 und G. 2713/1999 verwiesen, so dass eine begrenzte Dauer nach diesen Normen gilt. In Bezug auf die Hellenic FIU sieht lediglich Art. 30 G. 4557/2018 eine zeitliche Grenze für die Speicherung und Aufbewahrung von Unterlagen und Informationen zur Prävention, Aufklärung und Untersuchung vor. Die meldepflichtigen Personen dürfen Unterlagen und Informationen über eine Person solange aufbewahren, wie das Kundenverhältnis bzw. das Mandat dauert und darüber hinaus bis zu fünf Jahre nach Beendigung dieses Verhältnisses. Es besteht die Möglichkeit der Verlängerung der Frist bis auf zehn Jahre. Über eine Person können für die Dauer ihrer jeweiligen Geschäftsbeziehung (z. B. mit einer Bank) Informationen über ihre Vermögensverhältnisse oder Banktransaktionen gesammelt und verarbeitet werden, ohne dass sie je Kenntnis davon erlangt.

4. Ermittlungsschwelle

Für eine Maßnahme der Behörde genügt jede Information von den durch das G. 4557/2018 zur Meldung verpflichteten Personen, von den Strafverfolgungs- oder Justizbehörden im Rahmen eines Ermittlungsverfahrens oder Prozesses oder auch von Privaten. Darüber hinaus verfügt die Einheit C der Hellenic FIU als die zuständige Behörde für die Abgabe der Vermögenssteuerklärungen der dazu gesetzlich verpflichteten Personen über Informationen über die Vermögensverhältnissen von diesen Personen.

Art. 22 G. 4557/2018 führt die Pflicht zur Meldung einer verdächtigen Transaktion an die Behörde ein. Insbesondere sind die durch den Art. 5 G. 4557/2018 genannten Personen zur unverzüglichen und eigeninitiativen Meldung verpflichtet, wenn sie wissen oder ernste Hinweise oder einen Verdacht haben, dass eine Geldsumme eine Einkunft aus einer Straftat sein oder in Verbindung mit Terrorismusfinanzierung stehen könnte. Die Meldung muss nicht gesondert begründet sein und wird als „streng geheim“ eingestuft. Es genügt, wenn eine Transaktion einem

Bankangestellten außergewöhnlich oder verdächtigt erscheint, so z.B. nach Art. 38 § 1 S. 1 G. 4557/2018 hinsichtlich der Meldepflicht der Kredit- und Bankinstitute. Gem. Art. 3 Nr. 14 G. 4557/2018 ist eine Transaktion verdächtig, wenn für sie hinreichende Hinweise oder ein Verdacht bestehen, dass sie einen Versuch oder eine Tat der Geldwäsche oder der Terrorismusfinanzierung darstellen könnte. Für die Einschätzung nennt diese Norm verschiedene Kriterien, wie die Art, die Regelmäßigkeit, die Komplexität oder Höhe der Transaktion, die Einzahlung von Bargeld, der Beruf, die Vermögensverhältnisse, das geschäftliche Verhalten und die Vergangenheit der Person, etc. Gem. Art. 3 Nr. 15 G. 4557/2018 gilt eine Transaktion als außergewöhnlich, die mit dem geschäftlichen, beruflichen oder unternehmerischen Verhalten der Person oder des wahren Inhabers bzw. mit ihrem finanziellen Zustand nicht im Einklang steht. Außergewöhnlich ist eine Transaktion, die keinen offenkundigen Zweck oder Motive wirtschaftlicher, beruflicher oder persönlicher Natur zu haben scheint.

Festzustellen ist, dass die gesetzlichen Regelungen der Hellenic FIU viele Möglichkeiten einräumen, über finanzwirtschaftliche Informationen zu verfügen. Zum einen genügt jede Meldung für den Beginn der Ermittlungen durch die Hellenic FIU. Zum anderen sind, wie auch oben erwähnt, Strafverfolgung- und Justizbehörden gem. Art. 50 § 1 G. 4557/2018 verpflichtet, Informationen über Personen, die im Zusammenhang mit Terrorismus stehen, an der Hellenic FIU weiterzuvermitteln. Auch verfügt sie, namentlich durch die Einheit C, sowieso über Informationen über die Vermögensverhältnisse der zur Abgabe der Vermögenssteuerklärungen gesetzlich verpflichteten Personen, weil sie auch die zuständige Finanzbehörde dafür ist. Für ihre Ermittlungen muss nicht zwingend eine verdächtige Transaktion vorliegen. Es ist ausreichend, dass die Transaktion als außergewöhnlich erscheint, damit sie unter die Lupe genommen wird. Dies bedeutet, dass die Anforderungen für die Ermittlungen durch die Hellenic FIU niedriger sind als diese an einem Tatverdacht im Sinne der grStPO. Die Besonderheit bei der Hellenic FIU ist, dass sie keine polizeiliche Behörde wie die DiDAP ist und ihr Ermittlungsverfahren schwer in der Sicherheitsarchitektur des griechischen Staates eingeordnet werden kann.

D. Koordinationsmechanismen

Die Koordination der Tätigkeiten zwischen den Sicherheitsbehörden eines Staates ist eine unabdingbare Voraussetzung für die Effektivität ihrer Funktionen. Koordinationsmechanismen existieren auch in Griechenland sowohl auf Regierungsebene, allerdings eingeschränkt auf bestimmte Tätigkeitsfelder, wie auch innerhalb der jeweiligen Behörden. Ein zentraler Koordinationsmechanismus zwischen Nachrichtendiensten und Strafverfolgungsbehörden im Bereich der Verbrechensbekämpfung ist aber nicht vorhanden. Es ist nicht auszuschließen, dass in der Zukunft eine zentrale Koordinationsstelle für die innere und äußere Sicherheit des

Staates aufgebaut wird, etwa im Vorbild eines sog. „Nationalen Sicherheitsrates" wie in den USA.[38]

Im begrenzten Rahmen dieser Abhandlung genügt es, darauf hinzuweisen, dass in jeder Sicherheitsbehörde Stellen und Zentren vorgesehen sind, die der Koordination und Zusammenarbeit der einzelnen Abteilungen, Direktionen und Einheiten dienen. Die Zusammenarbeit erstreckt sich auf die effektive Erfüllung ihrer Aufgaben oder auch auf die Bekämpfung von Krisen. Exemplarisch sind zu erwähnen:

– Das Generalsekretariat für den Zivilschutz (Γενική Γραμματεία Πολιτικής Προστασίας, G.G.P.P.) als eine eigenständige Verwaltungsbehörde mit Koordinationsfunktion ist in Fällen von natürlichen, technologisch-bedingten und anderen Katastrophen oder Notzuständen sowie für die Bewältigung von chemischen, biologischen, radiologischen und Atom-Unfällen zuständig.
– Im Fall der Bedrohung der nationalen Sicherheit sowie im Fall eines Krieges ist der Regierungsrat für Außenverhältnisse und Verteidigung zuständig (Κυβερνητικό Συμβούλιο Εξωτερικών και Άμυνας, ΚΥΣΕΑ), bestehend aus dem Ministerpräsidenten sowie dem Außen- und Verteidigungsminister und dem Minister für Schifffahrt und Inselpolitik.
– Im Fall von schweren kriminellen Aktivitäten und Bedrohungen für die Sicherheit des Staates oder seiner Beziehungen mit anderen Staaten wird nach Art. 7 des G. 3649/2008 der sog. „Koordinationsrat für die Verwaltung von Informationen (Συντονιστικό Συμβούλιο Διαχείρισης Πληροφοριών)" aktiviert. Es handelt sich um einen Koordinationsmechanismus auf Regierungsebene. Der EYP beteiligt sich, indem er gem. Art. 7 § 4 G. 3649/2008 Sekretärsaufgaben erfüllt.
– Innerhalb des EYP ist der Informationsrat (Συμβούλιο Πληροφοριών) gem. Art. 8 des G. 3649/2008 für die Koordination aller Informationsdienste und Sicherheitsbehörden des Staates im Bereich der Sammlung und Zugänglichmachung von Informationen zuständig. Im Falle einer Aktivität mit dem Ziel der Auflösung der demokratischen Staatsform sieht Art. 2 § 2 S. 2 G. 3649/2008 vor, dass der EYP die zentrale Behörde für die Informationenverwaltung des Staates wird.
– Innerhalb der EL.AS. sind weitere Koordinationsmechanismen vorgesehen, z.B. auf Direktionsebene das Einheitliche Koordinationszentrum für Operationen und Verwaltung von Krisen, gem. Art. 21 G. 4249/2014, z.B. für die Bekämpfung von kritischen auch überregionalen Kriminalitätsfällen; der Koordinationsdienst für die Verwaltung von Krisen der inneren Sicherheit insbesondere für Fälle der terroristischen Angriffe und Bedrohungen gegen den Staat gem. Art. 61 des G. 4249/2014.
– Innerhalb der Hellenic FIU sind zwei Koordinationsmechanismen vorgesehen. Das Finanzministerium ist gem. Art. 7 G. 4557/2018 die zentrale Koordinations-

[38] Vgl. Vorschläge von *Mazis*, in: Staat – Sicherheit, 155 – 162; *Ntokos*, in: Staat – Sicherheit, 65, 72–73.

und Aufsichtsstelle. Die Kommission im Finanzministerium zur Entwicklung von Strategien der nationalen Reaktion ist gem. Art. 8 G. 4557/2018 für die Bekämpfung der Geldwäsche und der Terrorismusfinanzierung zuständig.

E. Anknüpfungspunkte für eine Operationalisierung der Nachrichtendienste für die Verbrechensbekämpfung

Nachdem oben die griechischen Nachrichtendienste überblicksweise vorgestellt wurden, wird im Folgenden der Frage nachgegangen, ob und inwiefern diese Dienste für die Verbrechensbekämpfung herangezogen werden. Die Analyse bezieht sich auf die Darstellung von Anhaltspunkten für die Operationalisierung der Nachrichtendienste für die Strafverfolgung sowie für die Operationalisierung der Polizei für nachrichtendienstliche Aufgaben. Diese Anhaltspunkte werden in drei Kategorien untergliedert: organisatorische Besonderheiten, Aufgabenfelder und Befugnisse.

1. Organisatorische Besonderheiten

Der EYP stellt gem. dem Wortlaut des Art. 1 G. 3649/2008 einen eigenständigen, zivilen, öffentlichen Dienst dar und ist gem. Art. 21 § 4 G. 4622/2019, Art. 5 §§ 3 und 5 PVO 81/2019 dem Premierminister untergeordnet. Dieser ist sein hierarchischer Vorgesetzter. Der EYP hat eine Struktur als selbstständige Verwaltungseinheit und ist auch eine der Sicherheitskörperschaften[39] des griechischen Staates. Die DiDAP hat eine gewisse administrative Selbstständigkeit, sie ist jedoch dem sog. Hauptquartier der Hellenischen Polizei (EL.AS.), in der sich ihre Leitung befindet, direkt untergeordnet. Die DiDAP untersteht somit über die EL.AS. dem Ministerium für den Bürgerschutz. Als der Informationsdienst der Hellenischen Polizei steht sie ebenfalls der Exekutive nahe. Dies gilt auch für die Hellenic FIU als eine selbstständige Verwaltungsbehörde. Sie genießt gem. Art. 47 § 2 S. 1 G. 4557/2018 administrative und funktionelle Unabhängigkeit und untersteht dem Finanzminister. Bei der Hellenic FIU besteht also einerseits die Besonderheit, dass sie ins Finanzministerium und nicht ins Ministerium für den Bürgerschutz eingegliedert ist, also nicht in das Ministerium, das typischerweise Aufsichtsbehörde der Sicherheitsbehörden des Staates ist. Andererseits ist sie eng mit dem Finanzsektor des griechischen Staates

---

[39] Die Sicherheitskörperschaft (Σώμα Ασφαλείας) als Institution wird auch im griechischen GG, z.B. in Art. 23 § 2 Fall β, Art. 29 § 2, Art. 56 §§ 1, 3, 4 grGG, erwähnt und anerkannt. Damit eine Institution als „Sicherheitskörperschaft" bezeichnet wird, müssen zwei Voraussetzungen kumulativ vorliegen: Sie muss als eine „Körperschaft" organisiert werden und ihre Aufgabe muss in der Sicherheit im Sinne der allgemeinen Polizei im engen Sinne (Γενική Αστυνόμευση) bestehen. In diesem Sinne stellt EL.AS. eine Sicherheitskörperschaft dar. Der EYP gehört aufgrund seiner Organisation, Struktur, Funktion und Tätigkeit auch zu den Sicherheitskörperschaften, vgl. *Alivizatos*, NoB 1983, 621, 625; *Papaioannou*, Polizeigewalt, S. 91; *Tachos*, öffentliche Ordnung, S. 126–127.

verbunden, namentlich unter anderem mit der „Bank of Greece“ und der „Griechischen Kommission des Kapitalmarktes“.

Die griechischen Nachrichtendienste weisen somit eine offensichtliche Nähe zur Exekutive auf und sind Teil der Ausübung der öffentlichen Verwaltung als Ausdruck der Regierungspolitik im Bereich der inneren öffentlichen Sicherheit und Ordnung. Die Eingliederung der Nachrichtendienste in der Sicherheitsarchitektur des Staates hat eine dreifache Bedeutung, nämlich unter den Aspekten: a) der politischen Verantwortung für ihre Tätigkeiten, b) der Verstärkung der Macht des vorgesetzten Ministers und c) der Leitlinien, die für ihre Tätigkeiten gelten.[40] So wäre z.B. die Unterordnung der Nachrichtendienste unter das Justizministerium zugleich ein Zeichen für die Unbefangenheit und stärkere Rechtmäßigkeit ihrer Funktion, ihre Unterordnung unter das Verteidigungsministerium ein Zeichen für ihre zentrale Rolle in der Verteidigungs- und Außenpolitik des Staates. Die Unterordnung unter den Minister für den Bürgerschutz ist daher ein Indikator der Kontrolle zum Schutz der Sicherheit der Bürger. Es ist ein Zeichen für einen mehr offensiven Charakter ihrer Tätigkeiten im inneren Sicherheitsbereich. Die Abkopplung des EYP vom Ministerium für den Bürgerschutz und seine Unterordnung direkt unter den Premierminister ist ein Indikator für die Stärkung der Position des Premierministers und seiner Macht. Zudem ist es ein Zeichen für die Hervorhebung einer besonderen Rolle des EYP sowohl in der äußeren wie auch in der inneren Sicherheit des griechischen Staates.

2. Kriminalitätsbereiche als Aufklärungsfelder der Nachrichtendienste

Die Nachrichtendienste werden in folgenden Kriminalitätsbereichen für die Aufklärung einer Straftat tätig:

1. Spionage und Staatsschutzdelikte: in Bezug auf diese Delikte, die eine Bedrohung für die nationale Sicherheit oder die demokratische Staatsorganisation sein können, ist der EYP gem. Art. 4 Nr. 1 G. 3649/2008 tätig.
2. Organisierte Kriminalität, Terrorismus und Geldwäsche, Illegale Einwanderung, Menschenhandel und Massenvernichtungswaffen. In diesem Bereich sind alle drei Nachrichtendienste tätig. Insbesondere:

   Gem. Art. 4 Nr. 2 G. 3649/2008 sammelt der EYP Informationen über die Aktivitäten terroristischer Organisationen oder anderer Gruppen organisierter Kriminalität im Bereich von illegalem Menschenhandel, illegalem Handel mit menschlichen Organen, mit Waffen, mit Drogen oder anderen verbotenen Stoffen, wie radioaktiven Stoffen und Kernmaterial, radiobiologischen und chemischen Stoffen. Er sammelt Informationen auch im Bereich der Geldwäsche. Die Aufzählung der Kriminalitätsbereiche im Wortlaut ist nicht abschließend, sondern

---

[40] Vgl. *Apostolidis*, EYP, S. 11 – 12.

exemplarisch.[41] Die Norm soll trotzdem restriktiv ausgelegt werden. Für einen Ausschluss der einfachen Kriminalität aus dem Bereich des EYP sprechen der schwerwiegende Charakter der dort aufgezählten Kriminalitätsbereiche sowie der Auftrag des EYP, die demokratische Staatsform und die nationale Sicherheit als solche vor schwerwiegenden Gefahren zu schützen.

In den Kriminalitätsfeldern der Geldwäsche, des Terrorismus und der Terrorismusfinanzierung beobachtet und sammelt auch die Hellenic FIU Informationen.

Gem. Art. 22 § 1 G. 4249/2014 fallen die Bekämpfung des Terrorismus und der organisierten Kriminalität in den Aufgabenbereich der DiDAP. Bei näherem Hinsehen lässt sich allerdings feststellen, dass die DiDAP darüber hinaus zur Informationssammlung hinsichtlich weiterer Straftaten befugt ist. Dies ergibt sich aus Art. 27 § 1 PVO 178/2014 i.V.m. Art. 2 lit. ε΄der PVO 135/2013[42]. Dabei handelt es sich um einen langen Katalog von Straftaten, insgesamt 31 Kategorien. Es sind nicht nur Straftaten der organisierten Kriminalität, sondern auch exemplarisch Urkundenstraftaten, Vergewaltigung, Totschlag/Mord, Brandstiftung, Umweltstraftaten, schwere Körperverletzung, organisierter oder bewaffneter Raub oder Diebstahl, IT-bezogene Straftaten etc. genannt. Auf diese Weise erweitert sich der Kriminalitätsbereich des polizeilichen Nachrichtendienstes enorm, bei dem diese durch Überwachung und Informationsbeschaffung tätig werden darf.

3. Cyberkriminalität: Mit der Benennung des EYP als INFOSEC-Stelle gem. Art. 4 § 7 G. 3649/2008 und als nationaler CERT gem. Art. 4 § 8 G. 3649/2008 ist er zur zentralen Stelle für die komplette Überwachung der informationstechnischen Systeme und Netzwerke des griechischen Staates geworden. Dabei ist der EYP nicht nur als die zentrale Zertifizierungs- und Bewertungsstelle aller Informationssysteme zuständig. Er ist auch die zentrale Stelle für die Bekämpfung – aktiv wie passiv – der Cyberkriminalität.

3. Erweiterungstendenzen

Aus dem Vergleich der derzeit für den EYP geltenden Rechtsnormen, namentlich des G. 3649/2008, mit dem alten G. 1645/1986 lässt sich eine erhebliche Erweiterung der Zuständigkeitsbereiche und Kompetenzen des EYP feststellen. Gem. Art. 2 des G. 1645/1986 war der EYP nur im Bereich der äußeren Sicherheit und die Bekämpfung der Spionage zuständig. Art. 2 § 1 Fall d) G. 1645/1986 sah auch die Möglichkeit vor, dass der EYP vom damaligen Sicherheitsrat oder Premierminister damit beauftragt wird, einen mit diesen Tätigkeitsbereichen zusammenhängenden Auftrag auszuführen. Diese Tätigkeit musste aber einen Zusammenhang mit der äußeren

---

[41] Vgl. den Wortlaut des Art. 4 § 2 G. 3649/2008 „κυρίως (grundsätzlich)".

[42] Zur Anpassung an dem Rahmenbeschluss 2006/960/JI des Rates vom 18. Dez. 2006 über die Vereinfachung des Austausches von Informationen und Erkenntnissen zwischen den Strafverfolgungsbehörden der Mitgliedstaaten der EU, ΦΕΚ/Α/209/30.9.2013.

Sicherheit aufweisen. Mit G. 3649/2008 erfolgte eine enorme Ausweitung der Tätigkeitsfelder des EYP. Diese Erweiterung des sachlichen Zuständigkeitsbereichs des EYP ist laut der Gesetzesbegründung[43] eine gerechtfertigte und notwendige Reaktion auf die aktuellen Bedrohungen für den Staat und die Sicherheit. Diese Bedrohungen beruhen auf Gefahren aus den weltweiten terroristischen Angriffen, aus der Cyberkriminalität, aus der Ausweitung der organisierten Kriminalität nicht nur im Bereich des Terrorismus, sondern auch in vielen anderen Kriminalitätsbereichen, z.B. beim Menschenhandel. Die PVO 1/2017 ersetzte die alte PVO 126/2009 über die Organisation des EYP. Die Behörde wurde umstrukturiert, ihr Personal wurde erweitert und neue Abteilungen wurden gegründet.

Auch die DiDAP ist eine junge wachsende Behörde. Im Hinblick auf den Terrorismus, die organisierte Kriminalität, die Wirtschaftskriminalität und die Geldwäsche lassen sich Überschneidungen mit den Tätigkeitsgebieten des EYP feststellen. Im Oktober 2017 ist die DiDAP von einem Stockwerk der Generaldirektion der EL.AS. in ein neues Gebäude umgezogen. Dies ist mehr als eine räumliche Veränderung. Die Direktion wächst nicht nur hinsichtlich des Personals, sondern auch bezüglich der technischen Ausstattung. Es ist ein Zeichen für ihre Verselbständigung. Mit dem technischen Wissen britischer Wissenschaftler entwickelt sie die modernste Technik für die Telekommunikationsüberwachung und für ein globales Positionsbestimmungssystem (GSP). Im neuen Gebäude verfügt sie auch über die informationstechnische Infrastruktur für die Aufzeichnung und Speicherung aller Flugdaten und Flugpassagierdaten (PNR).[44]

Schließlich ist durch die Gründung der Hellenic FIU ein weiterer Nachrichtendienst hinzugekommen, wobei der Antrieb dazu aus der internationalen sowie europäischen Politik zur Bekämpfung der Geldwäsche und des Terrorismus stammt. In Europa lässt sich dies an einer Reihe von Richtlinien festmachen.[45] Die Hellenic FIU wurde durch das G. 3932/2011 verselbständigt und umstrukturiert. Zuletzt wurde sie durch das G. 4557/2018 um weitere Stellen und Befugnisse, etwa in Bezug auf den Terrorismus (gem. Art. 50 des G. 4557/2018), ausgebaut.

Eine Operationalisierung im Sinne einer unmittelbaren Heranziehung der Nachrichtendienste für die Verbrechensbekämpfung ist in Griechenland zunächst nicht festzustellen. Auf der anderen Seite lässt sich aber konstatieren, dass alle drei Nachrichtendienste Informationen über Kriminalitätsbereiche sammeln und ermitteln, die sich nicht nur miteinander decken, sondern sich auch mit den Kriminalitätsbereichen

---

[43] Gesetzesbegründung zum G. 3649/2008, S. 1, abrufbar unter https://www.hellenicparliament.gr/UserFiles/2f026f42-950c-4efc-b950-340c4fb76a24/E-EYPL-EIS.pdf, [Stand: 20.12.2019].

[44] Veröffentlichte Informationen im Zeitungsartikel vom 02.09.2017, abrufbar unter: http://www.kathimerini.gr/924950/article/epikairothta/ellada/aytonomeitai-h-yphresia-plhroforiwn-ths-elas (auf Griechisch), [Stand: 20.12.2019].

[45] Die RL 2015/849/EU ist die vierte und letzte von einer Reihe von Richtlinien zur Bekämpfung der Geldwäsche und Terrorismus.

der Strafverfolgungsbehörden überschneiden. Die Nachrichtendienste sind für bestimmte Kriminalitätsbereiche parallel zu den normalen Strafverfolgungsbehörden tätig. Durch die DiDAP lässt sich auch eine Vernachrichtendienstlichung der Polizei vor allem im Rahmen der Prävention feststellen. Wenn diese Tendenz der Zunahme der Überschneidungen in den Kriminalitätsbereichen sowie der Erweiterung ihrer Eingriffsbefugnisse weiter verstärkt wird, wird nicht auszuschließen sein, dass die Nachrichtendienste faktisch bzw. mittelbar für die Verbrechensbekämpfung operationalisiert werden.

Teil 2: Interaktionen zwischen Nachrichtendiensten und Strafverfolgungsbehörden

Nicht nur die oben aufgeführten Erweiterungstendenzen und organisatorischen Besonderheiten (man denke z.B. an die organisatorische Einordnung der DiDAP in die Polizei), sondern auch die Kriminalitätsbereiche, in denen die Dienste operieren, weisen auf durchaus rege Wechselwirkungen zwischen den Nachrichtendiensten und Strafverfolgungsbehörden hin. Es stellt sich die Frage, ob das griechische Recht normative Vorgaben aufweist, die die genannten Wechselwirkungen regeln würden.

In der griechischen Rechtsordnung bestehen keine expliziten normativen Ansätze dafür, wie Nachrichtendienste und Strafverfolgungsbehörden interagieren sollen. Auch gibt es keinen allgemein anerkannten Grundsatz, der auf die Interaktionen zwischen Nachrichtendiensten und Strafverfolgungsbehörden regulativ bzw. korrektiv wirken würde. Von einem Trennungsgebot, wie es diesbezüglich in Deutschland gilt, ist weder im Schrifttum noch in der Rechtsprechung die Rede. Im Folgenden wird trotzdem zum Zwecke eines Rechtsvergleichs im Lichte des in Deutschland anerkannten Trennungsgebots die Rechtslage in Griechenland bewertet.

I. Trennungsgebot

Die Aufzählung von sonderpolizeilichen Behörden (Art. 87 Abs. 1 S. 2 GG) und von Gebieten der Zusammenarbeit zwischen Bund und Ländern (Art. 73 Abs. 1 Nr. 10 GG) im deutschen Grundgesetz indiziert eine Trennung zwischen den Sicherheitsbehörden in Deutschland.[46] In der Tat nimmt das BVerfG ein sog. Trennungsgebot an, das aus dem Rechtsstaatsprinzip, dem Bundesstaatsprinzip und dem Schutz der Grundrechte abgeleitet wird. Laut dem BVerfG[47] besagt das Trennungsgebot,

---

[46] Eine Ableitung des Trennungsgebots aus diesen Normen vertritt z.B. *Gusy*, ZRP 1987, 45, 46–48. Zum Trennungsgebot s. u.a. auch *Nehm*, NJW 2004, 3289, 3290–3292; *Zöllner*, JZ 2007, 763, 766–767.

[47] Vgl. BVerfGE 97, 198, 217.

dass es verboten ist, bestimmte Behörden zusammenzulegen oder mit Aufgaben zu beauftragen, die mit ihrer verfassungsrechtlichen Aufgabenstellung nicht vereinbar sind. Das Gericht erklärt weiter, dass die Zentralstellen für Zwecke des Verfassungsschutzes oder des Nachrichtendienstes angesichts von deren andersartigen Aufgaben und Befugnisse nicht mit einer Vollzugspolizeibehörde zusammengelegt werden dürfen.[48] Vielmehr muss zwischen Strafverfolgungsbehörden und Nachrichtendiensten eine funktionale, organisatorische, personelle und informationelle Trennung vorhanden sein. So hat das BVerfG-Urteil[49] zum Antiterrordateigesetz hervorgehoben, dass Regelungen, die den Austausch von Daten der Polizeibehörden und Nachrichtendienste ermöglichen, hinsichtlich des Grundrechts auf informationelle Selbstbestimmung gesteigerten verfassungsrechtlichen Anforderungen unterliegen. Aus den Grundrechten folgt ein informationelles Trennungsprinzip, das diesen Austausch nur ausnahmsweise zulässt.

Das Trennungsgebot besagt allerdings nicht, dass eine Zusammenarbeit zwischen Nachrichtendiensten und Polizei unzulässig sei. Es bestimmt nur die Art und die Bedingungen, wie diese Zusammenarbeit erfolgen darf.[50] Die Trennung impliziert jedoch eine organisatorische und informationelle Gewaltenteilung. Überschneidungen insbesondere im funktionellen Bereich darf es geben. Aber im gleichen Funktions- bzw. Sachgebiet dürfen Nachrichtendienste und Strafverfolgungsbehörden nicht die gleiche Art von Aufgaben, namentlich sowohl nachrichtendienstliche wie auch polizeiliche, wahrnehmen. Der Sinn und Zweck des Trennungsgebots liegt also gerade im Ausschluss der Nachrichtendienste von den polizeilichen Befugnissen.[51] Denn es besteht eine Gefahr für die Grundrechte, die rechtsstaatlichen und freiheitlichen Garantien der Verbrechensverfolgung, wenn das Wissen der Nachrichtendienste für die Ausübung von Polizeigewalt genutzt wird.[52]

II. Überlegungen zu einer funktionalen, organisatorischen und personellen Trennung im Sinne des Trennungsgebots

Im Folgenden wird untersucht, ob und inwieweit es eine funktionale, organisatorische und personelle Trennung zwischen den Nachrichtendiensten und den Strafverfolgungsbehörden im Sinne des Trennungsgebots in Griechenland gibt. Als Tendenz ist einerseits der zunehmende Einsatz der Nachrichtendienste im Bereich der Verbrechensbekämpfung, andererseits auch die Vernachrichtendienstlichung der

---

[48] Vgl. BVerfGE 97, 198, 217.

[49] BVerfG, Urteil v. 24.2.2013 – 1 BvR 1215/07, JZ 2013, 621–632.

[50] Vgl. *Gusy*, ZRP 1987, 45, 49.

[51] Vgl. *Gusy*, ZRP 1987, 45, 49.

[52] Hier ist bspw. an die bitteren Erfahrungen mit der Gestapo in Deutschland zu denken, vgl. u.a. *Kutscha*, ZRP 1986, 194 oder mit dem EYP während der griechischen Militärdiktatur, s. oben Fn. 19.

Polizei durch die DiDAP erkennbar. Aus der Beschreibung des modus operandi lässt sich feststellen, dass Nachrichtendienste unter bestimmten Voraussetzungen kriminalpolizeiliche Befugnisse ausüben dürfen. Die DiDAP agiert als nachrichtendienstliche Einheit der Polizei. Dies sind Indizien dafür, dass die funktionale Aufteilung zwischen den Sicherheitsbehörden schwach ist.

Insbesondere im Bereich des Terrorismus, der Geldwäsche und der Terrorismusfinanzierung operiert zusätzlich die Hellenic FIU neben dem EYP und der DiDAP. Eine Einschränkung könnte sich hier aus der finanziellen Natur der gesammelten Informationen ergeben, denn dieser Finanzinformationsdienst ist grundsätzlich auf die Überwachung der Vermögensverhältnisse und der Transaktionen von Personen beschränkt. Obwohl sie zur Verbrechensbekämpfung und somit zur inneren Sicherheit beiträgt, lässt sie sich schwer in die Sicherheitsarchitektur des Staates einordnen. Es handelt sich vielmehr um eine Art Mischbehörde: Sie ist zum einen ein administrativer Nachrichtendienst des Finanzsektors des Staates, der mit zusätzlich polizeilichen Aufgaben (Ermittlung, Durchsuchung, Beweissicherung, Sanktionsverhängung und Sanktionsvollzug) in Bezug auf Geldwäsche, Terrorismus und Terrorismusfinanzierung ausgestattet ist, obwohl sie keine echte Strafverfolgungs- oder Justizbehörde ist. Darüber hinaus ist sie mit finanzamtlichen Aufgaben betraut, namentlich ist sie die zuständige Finanzbehörde für die Annahme der Vermögensteuerklärungen von steuerpflichtigen Personen und die zentrale Meldestelle für verdächtige oder bloß außergewöhnliche Transaktionen eine sehr großen Gruppe meldepflichtiger Personen.

Eine starke personelle Trennung zwischen Nachrichtendiensten und Strafverfolgungsbehörden ist ebenfalls nicht vorhanden. Beim EYP sind neben dem zivilen Personal gem. Art. 10 G. 3649/2008 auch Offiziere und Unteroffiziere des Heers, der Hellenischen Küstenwache, der Feuerwehr sowie der EL.AS. tätig. Dieses Personal wird abgeordnet oder versetzt für einen Zeitraum von fünf Jahren mit der Möglichkeit einer Verlängerung ohne zeitliche Obergrenze (Art. 42 PVO 1/2017). Der Zeitraum für den Dienst beim EYP wird als Dienstzeit an der jeweiligen Behörde, aus der das Personal stammt, angerechnet, so Art. 18 G. 3649/2008. Beim EYP findet somit ein personeller Austausch mit den anderen Sicherheitsbehörden und mit dem Heer statt. Die DiDAP besteht aus Polizeibeamten, die grundsätzlich nachrichtendienstliche Tätigkeiten ausüben. Weder das G. 4249/2014 noch die PVO 178/2014 sehen einen besonderen Status für diese Beamten vor. Es besteht somit keine personelle Trennung zwischen diesem Nachrichtendienst und der Polizei, denn es handelt sich um den Nachrichtendienst der Polizei. Die Hellenic FIU besteht aus dem Präsident, 17 Mitgliedern und den Stellvertretern (Art. 47 § 4 G. 4557/2018). Die Dienstdauer beträgt drei Jahre mit der Möglichkeit der Verlängerung. Sie darf aber in keinem Fall sechs Jahre überschreiten. Gem. Art. 47 § 5 G. 4557/2018 ist der Präsident der Hellenic FIU ein Staatsanwalt der höchsten Ebene. Er wie auch sein Vertreter wird durch den Obersten Justizrat gewählt und ist an die Behörde für die Dauer seines Dienstes abgeordnet. Die Beschäftigten der Behörde werden durch einen gemeinsamen Beschluss unter anderem der Justiz-, Innen- und Außenminister, aber

auch des Direktors der Bank of Greece und des Vorstandes der Nationalen Kommission des Kapitalmarktes gewählt. Die Beschäftigten stammen aus unterschiedlichen Bereichen, z.B. aus dem Hauptquartier der EL.AS., der Bank of Greece, der Kommission des Kapitalmarktes usw.

Eine organisatorische und personelle Trennung kann nur anhand formaler Kriterien erfolgen. Es handelt sich um unterschiedliche Ämter, die unabhängig voneinander sind und als selbstständige Verwaltungseinheiten im Rahmen der Verbrechensbekämpfung tätig werden. Dabei ergeben sich Überschneidungen im Bereich der Spionage und der Staatsschutzdelikte, des Terrorismus, der organisierten Kriminalität und der Geldwäsche wie auch der Cyberkriminalität. In diesen Bereichen dürfen die Nachrichtendienste auch als Ermittlungsbehörden tätig werden, indem sie Ermittlungsaufgaben wahrnehmen, wie etwa Beweissicherung, Überwachung und verdeckte Ermittlungen. Auch der Personalaustausch zwischen den Sicherheitsbehörden mildert den Grad einer personellen Trennung. Besonders problematisch ist dann die Verschmelzung von Polizei und Nachrichtendienst im Fall der DiDAP.

III. Überlegungen zu einer informationellen Trennung im Sinne des Trennungsgebots

A. Informationsübermittlungsregelungen

Jede Sicherheitsbehörde sammelt zunächst eigene Informationen. Eine informationelle Zusammenarbeit ist in Deutschland in Anbetracht des Trennungsgebots an sich nicht unzulässig, solange kein durchgehend ungehinderter Informationsaustausch zwischen den Nachrichtendiensten und den Strafverfolgungsbehörden stattfindet. Außerdem wird hervorgehoben, dass die Art der Informationen und die Zwecke der Informationsbeschaffung unterschiedlich sind. Nachrichtendienste sollen Informationen grundsätzlich für sicherheitspolitische Zwecke und für einen begrenzten Sachbereich sammeln. Für die Nachrichtendienste gelten niedrigere Ermittlungsschwellen als für die Strafverfolgungsbehörden. Sie werden aktiv im „Vorfeld" einer Gefahrlage, eines Hinweises, eines Verdachts einer Straftat. Nachrichtendienste verfügen über „Vorfeldkenntnisse"[53]. Die Nutzung solcher Kenntnisse zum Zweck der Gefahrenabwehr oder der Strafverfolgung, die gerade durch die Verschmelzung der Nachrichtendienste und der Strafverfolgungsbehörden besonders leicht ist, erhöhen die Eingriffsintensität in die Rechte einer Person.[54]

Aus diesem Grund sind formale Voraussetzungen, wie der Informationsaustausch auf einen begründeten Antrag hin sowie das Einräumen eines Ermessenspielraums

---

[53] Vgl. *Gusy*, ZRP 1987, 45, 50. Zur informationellen Zusammenarbeit und Trennungsgebot s. auch *Kutscha*, ZRP 1986, 194, 196–197.

[54] Vgl. *Gärditz*, JZ 2013, 633, 634.

für den Nachrichtendienst hinsichtlich des Ob und des Umfangs der Informationsübermittlung von großer Bedeutung. Als Minimalanforderung verlangt das informationelle Trennungsgebot die Einführung von Normen, die eine gesetzliche Grundlage für einen Informationsaustausch zwischen den Nachrichtendiensten und den Strafverfolgungsbehörden im Inland wie im Ausland darstellen. Solche Normen können Übermittlungspflichten begründen. Sie sind Ermächtigungsgrundlagen für die Zulässigkeit der Übermittlung von Informationen an Dritte und zugleich gesetzliche Grundlage für den Antrag auf Informationen und die Begründung einer Übermittlungspflicht.

Im Fall des EYP sind den gesetzlichen Grundlagen keine ausführlichen Regelungen für die Informationsübermittlung zu entnehmen. Art. 6 G. 3649/2008 begründet eine allgemeine Pflicht für alle öffentlich-rechtlichen Behörden, Organisationen, Juristischen Personen des Öffentlichen Rechts, u.a. dem EYP jede Information, die wichtig für die Erfüllung seiner Aufgaben ist, auf Antrag zu übermitteln. Diese Norm stellt zum einen eine Grundlage für die zulässige Stellung eines Antrags auf Informationen durch den EYP dar. Zum anderen ist sie eine Grundlage für die Verpflichtung dieser Personen, Informationen an den EYP zu übermitteln. Die Ablehnung oder die Nichtleistung der beantragten Information ist ein Disziplinarvergehen. Wie diese Informationsübermittlung seitens öffentlich-rechtlicher Behörden an den EYP stattfindet, wird im Gesetz nicht geregelt. Vorausgesetzt wird ein schriftlicher Antrag des zuständigen bevollmächtigten Beamten des EYP. Im Übrigen unterscheidet der Areios Pagos[55] (AP) zwischen zwei weiteren Fällen. Beantragt der EYP Informationen mündlich oder beantragt er Abschriften von Akten, müssen die Strafverfolgungsbeamten diese Informationen an den EYP unter Einhaltung der Vertraulichkeit übermitteln. Auch der Antrag des EYP wird geheim gehalten und wird nicht Bestandteil der Akte. Selbst die Strafverfolgungsbeamten dürfen den zuständigen Staatsanwalt über den Antrag zum Zwecke der Geheimhaltung nur mündlich informieren. Des Weiteren hat der EYP die Befugnis, die Kontaktaufnahme mit einem Angeklagten zu beantragen. Die Rechtsmäßigkeit dieses Antrags prüft der zuständige – zum EYP abgeordnete – Staatsanwalt nach Art. 5 § 3 G. 3649/2008 und genehmigt bejahendenfalls den Antrag schriftlich, vorausgesetzt, dass die Einhaltung der Angeklagtenrechte gewährleistet wird. Sowohl der Antrag als auch die Kontaktaufnahme müssen geheim gehalten werden. Auch hier dürfen die Strafverfolgungsbehörden den örtlich zuständigen Staatsanwalt nur mündlich informieren. Die Kontaktaufnahme des EYP mit dem Angeklagten erfolgt ausschließlich zum Zwecke der nachrichtendienstlichen Informationssammlung und ist nicht als eine Ermittlungshandlung im Sinne der StPO zu qualifizieren. Eine Übermittlungspflicht des EYP von Amts wegen an die Strafverfolgungsbehörden ist im Gesetz ausdrücklich nicht vorgesehen. Er ist jedoch verpflichtet, mit anderen Behörden im Inland wie im

[55] AP 7/2014, Gutachten vom Staatsanwalt, unter www.areiospagos.gr, zuletzt besucht am 20.12.2019. Der Areios Pagos (Άρειος Πάγος AP) ist das höchste Gericht für Straf- und Zivilsachen in Griechenland. Er entspricht dem deutschen BGH.

Ausland zur Erfüllung der Aufgaben dieser Behörde informatorisch zusammenzuarbeiten, Art. 4 G. 3649/2008, z.B. mit den für die Krisenbekämpfung zuständigen staatlichen Behörden (Art. 4 § 5 G. 3649/2008) oder dem Verteidigungsministerium (Art. 4 § 6 G. 3649/2008). Art. 4 § 10 G. 3649/2008 sieht zudem die Aufgabe der Erstellung von Berichten und Informationsblättern vor, die der EYP dann an den zuständigen Behörden weiterleitet. Aus diesem gesetzlichen Rahmen ergibt sich eine allgemeine Pflicht des EYP zur Zusammenarbeit mit anderen Behörden. Deswegen ist es auch nicht auszuschließen, dass die Pflicht zur Zusammenarbeit des EYP auch die Pflicht zur Zusammenarbeit mit den Strafverfolgungsbehörden umfasst. Allerdings scheint das Gesetz es dem EYP zu überlassen, wann und wie er diese Pflicht erfüllt. Dem EYP steht insofern ein gewisser Ermessensspielraum zu.

Art. 22 § 2 G. 4249/2014 und Art. 27 § 10 PVO 178/2014 begründen die Pflicht für alle Abteilungen, Dienste und Einheiten der EL.AS. an die DiDAP unverzüglich alle Informationen weiterzuleiten, die sie im Rahmen ihrer Operationen sammeln. Die DiDAP tauscht Informationen auch mit anderen Einheiten der EL.AS. aus, etwa mit der Direktion für die Bekämpfung Spezieller Gewaltverbrechen (Διεύθυνση Αντιμετώπισης Ειδικών Εγκλημάτων Βίας, Δ.Α.Ε.Ε.Β.) gem. Art. 29 § 7 S. β PVO 178/2014,[56] mit der polizeilichen Einheit für die Bekämpfung der Cyberkriminalität gem. Art. 31 § 7 PVO 178/2014 oder der für die Bekämpfung der Wirtschaftskriminalität gem. Art. 32 § 12 PVO 178/2014. Des Weiteren kooperiert die DiDAP gem. Art. 11 § 7 lit. δ G. 4249/2014 und Art. 27 § 2 lit. β PVO 178/2014 zur effektiven Erfüllung ihrer Aufgaben mit internationalen Verbrechensbekämpfungsbehörden im Bereich des Informationsaustausches, z.B. mit Interpol, Europol etc. EL.AS. ist eine öffentlich-rechtliche Behörde, daher kann sie auf der Grundlage des Art. 6 G. 3649/2008 mit dem EYP auf der Ebene des Informationsaustausches zusammenarbeiten. Ob die DiDAP einen Ermessensspielraum bei der Übermittlung von Informationen an andere nationale wie auch internationale Strafverfolgungsbehörden hat, ergibt sich aus dem Wortlaut der gesetzlichen Regelungen nicht. Art. 27 § 2 lit. β PVO 178/2014 regelt, dass die DiDAP auf den Antrag auf Informationen seitens dieser Behörden hin Informationen im Verfahren und unter den Voraussetzungen übermittelt, die in einer internen Verordnung geregelt werden. Die interne Verordnung ist nicht veröffentlicht. Angesichts der Tatsache, dass die DiDAP nicht bloß Informationen sammelt, sondern vielmehr diese nach ihrer Wichtigkeit analysiert und nach Sicherheitsgrad einstuft, hat sie zumindest hinsichtlich dieser Bewertung der Informationen einen gewissen Ermessensspielraum.

Art. 5 G. 4557/2018 sieht einen langen Katalog der meldepflichtigen Personen vor, die gem. Art. 22 G. 4557/2018 verpflichtet sind, jede verdächtige oder außer-

---

[56] Die Aufgabe dieser Direktion besteht in der Bekämpfung von Gewaltverbrechen insbesondere von terroristischen und extemistischen Organisationen, insbesondere in der Bekämfung des inneren und äußeren Terrorismus sowie der Kriminalität gegen den Staat und die demokratische Staatsform, gem. Art. 17 § 9 G. 4249/2014, Art. 29 § 1 PVO 178/2014.

gewöhnliche Transaktion bzw. Vermögensänderung an die Hellenic FIU zu melden. Dies betrifft beispielsweise Steuerberater, Bank- und Kreditinstitute, Rechtsanwälte und Immobilienmakler. Insbesondere in Terrorismusfällen sind auch die Strafverfolgungs- und Justizbehörden gem. Art. 50 § 1 G. 4557/2018 verpflichtet, Informationen über Personen, die im Zusammenhang mit Terrorismus stehen, an die Hellenic FIU zu übermitteln. Die Hellenic FIU verfügt in sehr weitem Umfang über informatorische Befugnisse. Art. 34 § 2 G. 4557/2018 sieht die Informationsaustauschmöglichkeit zwischen der Hellenic FIU und anderen internationalen FIUs entweder aus eigener Initiative oder auf deren Antrag vor. Die Anträge müssen die Schilderung des Sachverhalts, den Untersuchungs- und Ermittlungsrahmen sowie die Art der Informationsnutzung umfassen. Insbesondere Art. 34 G. 4557/2018 regelt den Informationsaustausch zwischen der Hellenic FIU und anderen Behörden. Art. 34 § 1 G. 4557/2018 bestimmt, dass die Hellenic FIU an Strafverfolgungsbehörden sowie an Aufsichtsbehörden vertrauliche Informationen der meldepflichtigen Personen über Geldwäsche und Terrorismusfinanzierung übermitteln darf, solange diese Informationen für ihre Ermittlungen und die Erfüllungen ihrer Aufgaben als notwendig erachtet werden. Die Hellenic FIU darf die Übermittlung von Informationen insbesondere aus den im Gesetz genannt Gründen ablehnen.[57] Umgekehrt darf sie von diesen Behörden auch Informationen über die Ergebnisse ihrer Ermittlungen verlangen. Wenn die Hellenic FIU eine Vermögenssperre verhängt, dann ist sie verpflichtet, dies innerhalb von zwei Werktagen an die oberste Finanzverwaltungsbehörde zu melden (Art. 34 § 1 G. 4557/2018).

Des Weiteren ist die Hellenic FIU gem. Art. 34 § 5 G. 4557/2018 befugt, Memoranda über die informationelle Zusammenarbeit mit anderen Organisationen im In- oder im Ausland abzuschließen. Die Strafverfolgungsbehörden haben gem. Art. 44 G. 4557/2018 im Rahmen ihrer Ermittlungen Zugang zu den Archiven und den Informationen der meldepflichtigen Personen. Gem. Art. 49 § 1 G. 4557/2018 haben die Einheiten der Hellenic FIU Zugang über direkte Verbindungen, soweit diese möglich sind, zu jedem elektronischen Informationssystem und jeder Datenbank jeder öffentlichen Behörde oder Organisation. Strafverfolgungs- und Gerichtsbehörden übermitteln an die Hellenic FIU Informationen über Personen, die im Zusammenhang mit Terrorismus stehen, damit diese eine Liste dieser Personen gem. Art. 50 § 1 G. 4557/2018 führen kann. Insbesondere sind an die Hellenic FIU Informationen über die Anklageerhebung und Gerichtsurteile für die Verurteilung einer Person zum Terrorismus oder Terrorismusfinanzierung zu übermitteln. Dagegen regelt Art. 42 § 5 des G. 4557/2018, dass nach dem Abschluss einer Untersuchung die Hellenic FIU entscheiden darf, ob die Akte an die Staatsanwaltschaft weiterübermittelt oder ob sie nur archiviert wird. Es besteht somit keine Pflicht zur Übermittlung der Information an die Staatsanwaltschaft, sondern dies liegt im eigenen freien Ermessen der Hellenic FIU. Die Hellenic FIU darf die verdächtigen Personen nach

---

[57] Siehe auch unten Teil 2. III.B.

Informationen fragen. Im Rahmen ihrer Tätigkeit der Überprüfung eines Verdachts gilt das Steuer-, Berufs- und Bankgeheimnis ihr gegenüber nicht, es sei denn, es handelt sich um Berufsgeheimnisse von bestimmten Zeugenkategorien, z.B. Pfarrer, Ärzte oder Rechtsanwälte, die aufgrund ihrer beruflichen Tätigkeit Kenntnis von den verlangten Informationen erlangt haben (Art. 49 § 4 G. 4557/2018.) Aus diesen gesetzlichen Regelungen ergibt sich ein nicht begrenzter Ermessenspielraum für die Hellenic FIU hinsichtlich der Bewertung und der Entscheidung über das Ob und Wie der Weitergabe der Informationen, die sie sammelt.

B. Beschränkung der Übermittlungen

Die Informationsübermittlung zwischen den Sicherheitsbehörden erfolgt nicht unbeschränkt. Zwar enthalten die Gesetzen keine ausdrücklichen Übermittlungsverbote für die griechischen Nachrichtendienste und Strafverfolgungsbehörden; die Einschränkung der Informationsübermittlung erfolgt jedoch durch das Recht der Nachrichtendienste, die Übermittlung im eigenen Ermessen abzulehnen und somit dem Antrag einer Behörde aus bestimmten Gründen nicht nachzukommen. Zum anderen sind Geheimschutzpflichten für das Personal der Nachrichtendienste gesetzlich geregelt.

Eine allgemeine Pflicht der Nachrichtendienste, einen Fall bzw. Informationen an die Strafverfolgungsbehörden, etwa an die Staatsanwaltschaft, weiterzuleiten, ist in den gesetzlichen Regelungen über den jeweiligen Nachrichtendienst nicht enthalten. Eine solche Pflicht könnte sich aus Art. 38 grStPO ergeben. Art. 38 § 2 grStPO regelt die Pflicht aller Beamten und Angestellten im öffentlichen Dienst, jede im Rahmen ihrer Tätigkeit erhaltene Information über eine Straftat, die von Amts wegen verfolgt wird, an die Strafverfolgungsbehörden weiterzuleiten. Für die Informationsweiterleitung müssen hinreichende Hinweise auf eine Straftat vorliegen, wobei die Anforderungen an den Hinweis in diesem Sinne jedoch nicht so hoch sind wie bei einem Tatverdacht für eine Anklageerhebung.[58] Auch für die Beamten der EYP, DIDAP und Hellenic FIU gilt diese Pflicht grundsätzlich. Allerdings wird angenommen, dass diese Pflicht keinen absoluten Charakter hat. Die Nichtübermittlung einer Information über eine Straftat kann durch ein überwiegendes öffentliches Interesse gerechtfertigt sein.[59] Wie oben dargestellt räumt der griechische Gesetzgeber insbesondere der Hellenic FIU sogar ein Ermessen über die Entscheidung ein, ob nach Abschluss einer Untersuchung die Akte an die Strafverfolgungsbehörde übermittelt oder nur archiviert wird.

Für den EYP sieht Art. 14 G. 3649/2008 eine Geheimhaltungspflicht des Direktors, des stellvertretenden Direktors sowie des Personals vor. Die Geheimhaltungs-

---

[58] Vgl. *Androulakis*, Grundbegriffe, S. 269 Rn. 420.

[59] Vgl. *Androulakis*, Grundbegriffe, S. 269 Rn. 418.

pflicht gilt für alle Schriften, Informationen und Daten, von denen das Personal im Rahmen seiner Aufgaben Kenntnis erlangt. Die Verletzung der Geheimhaltungspflicht stellt ein Disziplinarvergehen wie auch eine Straftat (Art. 252 grStGB) dar. Für Informationen, die als geheim eingestuft worden sind, gilt die Geheimhaltungspflicht auch nach Beendigung des Dienstverhältnisses mit dem EYP. Art. 14 § 4 G. 3649/2008 i.V.m. Art. 5 § 5 PVO 81/2019 sieht für das Personal des EYP das Verbot vor, als Zeugen gegenüber den Strafverfolgungsbehörden oder Gerichten ohne eine vorherige Genehmigung seitens des Premierministers auszusagen. Auch Art. 14 § 5 G. 3649/2008 sieht die Möglichkeit vor, dass der EYP von den allgemeinen Übermittlungspflichten an andere Behörden ausgenommen werden kann, wenn nach Einschätzung des Direktors die Übermittlung das öffentliche Interesse schädigen wird. In diesem Fall darf der EYP einem Antrag auf Herausgabe von Informationen seitens einer anderen Behörde nicht stattgeben. Zugang zum Archiv und der Datenbank des EYP hat nur das Personal, das zu seiner Verwahrung und Verarbeitung besonders berechtigt ist.

Auch für die DiDAP gelten Geheimhaltungspflichten. Art. 27 § 7 PVO 178/2014 sieht eine Geheimhaltungspflicht für das Personal der DiDAP vor, deren Verletzung nach Art. 252 grStGB zum strafrechtlichen Schutz von Dienstgeheimnissen eine Straftat darstellt. Ebenfalls sind bei einer Verletzung der Geheimhaltungspflicht zivilrechtliche sowie disziplinarrechtliche Haftung gem. den entsprechenden Normen möglich. Neben der allgemeinen Klausel für die Zusammenarbeit und den Informationsaustausch zwischen der DiDAP und anderen externen Behörden bzw. anderen Abteilungen und Behörden innerhalb der Polizei enthalten die Normen keine Regelungen bezüglich des Informationsaustausches. Eine Einschränkung der Informationsverarbeitung durch die DiDAP ergibt sich aus der Pflicht zum Schutz personenbezogener Daten und des Kommunikationsgeheimnisses.

Der Präsident, das Personal und die Mitglieder der Hellenic FIU sind gem. Art. 49 § 7 G. 4557/2018 zur Geheimhaltung in Bezug auf Informationen verpflichtet, die sie im Rahmen ihrer Aufgabenerfüllung erlangen. Diese Geheimhaltungspflicht gilt auch gesetzlich unbegrenzt nach dem freiwilligen oder nicht freiwilligen Austritt aus der Behörde. Die Verletzung dieser Pflicht stellt eine Straftat dar, die mit Freiheitsstrafe von mindestens drei Monaten bestraft wird.

Etwas ausführlicher wird der Umgang der Hellenic FIU mit den gesammelten Informationen und Daten normiert. Die meldepflichtigen Personen sind verpflichtet, alle Daten und Informationen über die Personen zu speichern, mit denen sie ein Geschäftsverhältnis haben. Art. 30 § 3 G. 4557/2018 regelt über diese Speicherungspflicht Folgendes: Die Speicherungspflicht gilt zunächst für den Zeitraum der Dauer des Geschäftsverhältnisses. Darüber hinaus erstreckt sie sich auf eine Dauer von fünf Jahren nach Beendigung des Geschäftsverhältnisses. Dieser Zeitraum darf mit entsprechender Begründung verlängert werden, er darf aber die Dauer von zehn Jahren nicht übersteigen. In diesem Zeitraum sind alle gespeicherten Informationen der Hellenic FIU auf Antrag zur Verfügung zu stellen (Art. 30 §§ 1, 2, 4 G. 4557/2018).

In Bezug auf die Verarbeitung der personenbezogenen Daten regelt Art. 31 G. 4557/2018 i.V.m. dem G. 2472/1997 zum Schutz von personenbezogenen Daten, dass diese Verarbeitung nur zum Zweck der Prävention der Geldwäsche und der Terrorismusfinanzierung möglich und zulässig ist.

Die Hellenic FIU darf Informationen an Aufsichts- und Strafverfolgungsbehörden übermitteln, wenn diese Informationen für die Erfüllung der Aufgaben dieser Behörden notwendig sind. Sie darf in diesem Fall die Informationsübermittlung ablehnen, wenn diese ihre Ermittlungen gefährden oder verhindern würde oder sie deutlich unverhältnismäßig gegenüber den rechtmäßigen Interessen der betroffenen Person ist. Sie kann auch die Informationsübermittlung ablehnen, wenn dadurch die nationale Sicherheit gefährdet wird oder sie eine Menschenrechtsverletzung darstellt (Art. 34 § 3 G. 4557/2018). Auch ist die Behörde ermächtigt, gem. Art. 34 § 4 S. 1 G. 4557/2018 einschränkende Auflagen hinsichtlich der Verwendung der Informationen, die die Behörde an andere FIUs der EU-Staaten übermittelt, aufzuerlegen.

Art. 34 § 4 S. 2–5 G. 4557/2018 regelt den Fall der Weiterverwendung von schon übermittelten Informationen für andere Zwecke als die Zwecke der beantragten Übermittlung. Informationen, die der Hellenic FIU von den FIUs anderer Staaten und von anderen Behörden zur Verfügung gestellt werden, dürfen grundsätzlich nur zu den Zwecken verwendet werden, für die die Informationsübermittlung beantragt wurde. Die Verwendung dieser Informationen für andere als die beantragten Zwecke ist grundsätzlich nicht zulässig und bedarf der Genehmigung der übermittelnden FIU bzw. Behörde. Gleiches gilt auch umgekehrt: Die Weiterverwendung der Informationen, die die Hellenic FIU anderen FIUs oder Behörden übermittelt hat, für andere als die beantragten Zwecke bedarf auch ihrer Genehmigung. In diesem Fall darf die Hellenic FIU nur dann die Genehmigung der Weiterverwendung ablehnen, wenn drei Gründe alternativ oder kumulativ vorliegen: Erstens, wenn die Informationsübermittlung dem Anwendungsbereich der Rechtsnormen über die Prävention von Geldwäsche und Terrorismusfinanzierung nicht unterfällt. Zweitens, wenn die Informationsübermittlung ein Hindernis für eine inländische strafrechtliche Ermittlung darstellt oder einen unverhältnismäßigen Schaden legaler Interessen einer Person oder des öffentlichen Interesses begründet. Drittens, wenn die Informationsübermittlung gegen rechtsstaatliche Grundsätze verstößt. Eine Ablehnung der Genehmigung muss deswegen entsprechend begründet sein.

Nach der obigen Darstellung lässt sich feststellen, dass sie Übermittlung der nachrichtendienstlichen Informationen an die Strafverfolgungsbehörden grundsätzlich möglich ist. Die griechischen Nachrichtendienste verfügen sogar über einen gewissen Ermessenspielraum, wann und wie diese erfolgen soll. Daraus ergibt sich die Frage nach der strafprozessualen Zulässigkeit dieser Informationen vor den griechischen Strafgerichten. Im Folgenden ist vor allem zu untersuchen, ob und unter welchen Voraussetzungen diese Informationen in einem Gerichtsverfahren gegen eine Person verwendet werden dürfen.

C. Strafprozessuale Zulässigkeit der nachrichtendienstlichen Informationen

Im Rahmen der Untersuchung der informationellen Trennung zwischen Nachrichtendiensten und Strafverfolgungsbehörden wird die Frage aufgeworfen, ob und wie die nachrichtendienstlichen Informationen im Strafverfahren genutzt werden können. Gesetzlich geregelt sind nur zwei Fälle. Im ersten Fall geht es um die strafprozessuale Zulässigkeit von Material als Beweismittel, das durch eine Telekommunikationsüberwachung erhoben worden ist, unabhängig davon, ob diese Maßnahme durch die Strafverfolgungsbehörden oder durch die Nachrichtendienste erfolgt. Im zweiten Fall handelt es sich um die strafprozessuale Zulässigkeit der Vernehmungen von Beamten des EYP als Zeugen.

Die grStPO enthält Regelungen bezüglich der Erhebung von Beweisen im Ermittlungsverfahren wie auch der Verwendung dieser Beweise in der Hauptverhandlung vor Gericht. Diese Regelungen gehen aber auf die Problematik der Verwendung nachrichtendienstlicher Informationen im Strafverfahren nicht ein. Mit anderen Worten befasst sich das griechische Strafprozessrecht mit dem Phänomen der nachrichtendienstlichen Informationen nicht explizit. So ist nicht gesetzlich geregelt, ob und unter welchen Voraussetzungen die Nachrichtendienste zum Schutz ihrer Geheimnisse bei der Beweiserhebung das Ergreifen besonderer Maßnahmen fordern können, etwa eine Anonymisierung der Zeugen, die Nutzung von Beweissurrogaten, das Schwärzen von Dokumenten oder die Abhaltung eines In-camera-Verfahrens.

So orientiert sich beispielsweise die Einführung von Dokumenten und Schriften der Nachrichtendienste in das Ermittlungs- wie auch in das Hauptverfahren an den allgemeinen Beweisregeln über die Schriften in der grStPO. Insbesondere sieht Art. 263grStPO die Pflicht aller Beamten bzw. Personen des öffentlichen Dienstes vor – darunter also auch der Beamten der Nachrichtendienste – alle Daten, Schriften und Dokumente, die sie aufgrund ihrer Tätigkeit besitzen, den Strafverfolgungsbehörden auf deren Antrag hin abzuliefern. Von dieser Pflicht sind sie allerdings befreit, wenn sie sich (auch ohne besondere Begründung) schriftlich darauf berufen, dass es sich bei den angefragten Informationen bzw. Schriften um ein diplomatisches oder militärisches Geheimnis in Bezug auf die nationale Sicherheit oder um ein berufliches Geheimnis handelt.

Davon abgesehen kann sich also die strafprozessuale Zulässigkeit von nachrichtendienstlichen Informationen im Verfahren aus den allgemeinen Regelungen des Beweisrechts ergeben.

1. Zwei geregelte Fälle

a) Strafprozessuale Zulässigkeit der Beweismittel durch Telekommunikationsüberwachung gem. Art. 6 § 4 G. 2713/1999 und Art. 5 § 9 G. 2225/1994

Wie schon oben dargestellt,[60] sind die Informationssammelmethoden der Nachrichtendienste vielfältig. Eine der meist verbreiteten Ermittlungsmethoden der Nachrichtendienste ist wohl die Telekommunikationsüberwachung. Deswegen werden sich die folgenden Ausführungen auf diese Maßnahme beschränken. Im Jahr 2018 ergingen 11.113 staatsanwaltliche Anordnungen (Vorjahr 2017: 7.182 und im Jahr 2016: 9.295) und 3.400 Justizbeschlüsse der Strafverfolgungsbehörden (Vorjahr 2017: 3.194 und im Jahr 2016: 2947) über die Aufhebung des Kommunikationsgeheimnisses und die Anwendung von Überwachungsmaßnahmen.[61] In der Statistik wird nicht ausdrücklich zwischen nachrichtendienstlicher und strafprozessualer Telekommunikationsüberwachung differenziert. Für die Telekommunikationsüberwachung durch die Nachrichtendienste wird eine staatsanwaltliche Anordnung vorausgesetzt. Deswegen ist davon auszugehen, dass sich die Anzahl der staatsanwaltlichen Anordnungen in der Statistik auf die nachrichtendienstliche Telekommunikationsüberwachung bezieht. Die Anzahl der Justizbeschlüsse bezieht sich dann auf die Telekommunikationsüberwachung durch die Strafverfolgungsbehörden. Interessanterweise ist zu bemerken, dass 17,3 % der Justizbeschlüsse eine ortsbezogene flächendeckende Überwachung anordneten, die eine unbestimmte Anzahl von Personen betraf, die sich für die Dauer der Maßnahme an dem Ort befanden. Die staatsanwaltlichen Anordnungen betreffen Fälle der nationalen Sicherheit, die Beschlüsse betreffen Ermittlungen zur Aufklärung von Verbrechen, wie etwa Totschlag/Mord, Raub, Urkundenfälschung, Erpressung, organisierte Kriminalität, Drogenkriminalität u.a. Dies ist keine an sich verwerfliche Praxis, vor allem wenn es um schwere Kriminalität geht. Sie ist nur dann gefährlich, wenn die Grundrechte und die rechtsstaatlichen Garantien nicht beachtet werden. Deswegen müssen die Voraussetzungen, die in Art. 19 § 1 S. 2 grGG, in Art. 254 grStPO, in Art. 3, 4, 5 des G. 2225/1994 i.V.m. Art. 12 G. 3115/2003 über die Aufhebung des Kommunikationsgeheimnisses und in Art. 6 G. 2713/1999 über die technische Aufzeichnung und Überwachung der Aktivität und der Kommunikation einer Person geregelt werden, eingehalten werden.

Über die Beweisverwertungsnormen des grGG und der grStPO hinaus sieht Art. 6 § 4 G. 2713/1993 vor, dass aufgezeichnetes Material, das durch Überwachungsmaßnahmen nach der Aufhebung des Kommunikationsgeheimnisses gem. dem gesetzlichen Verfahren erhoben wurde, als zulässiges Beweismittel gilt und vor Gericht, von Strafverfolgungsbehörden und jeder anderen öffentliche Behörde verwendet werden darf. Auch Art. 5 § 9 S. 2 G. 2225/1994 sieht vor, dass das Material, das durch die

---

[60] S. in Teil 1. II. die jeweiligen Abschnitte über den Modus Operandi.

[61] Vgl. den Jahresbericht 2019 von ADAE, S. 51–52, abrufbar unter http://www.adae.gr/ektheseeis-pepragmenon/, [Stand: 20.12.2019].

Aufhebung des Kommunikationsgeheimnisses gesammelt werden konnte und der Aufklärung einer begangenen Straftat dient, Bestandteil der Akte für das Ermittlungsverfahren und die Hauptverhandlung wird. Als zulässiges Beweismittel gilt dieses Material sowohl im Ermittlungsverfahren wie auch in der Hauptverhandlung vor Gericht. Aufgrund dessen, dass das Material unter diesen Bedingungen auch von den Nachrichtendiensten erhoben werden kann, ist diese Klausel im Hinblick auf das Trennungsgebot nicht unproblematisch. Es muss eine Möglichkeit für die Prüfung der materiellen Rechtmäßigkeit einer solchen Erhebung durch das Strafgericht erhalten bleiben. Es genügt nicht, dass die formalen Voraussetzungen des Art. 6 G. 2713/1999 erfüllt werden. Auch die gesetzlichen Anforderungen an die Begründung der Maßnahme sind nicht hoch. Die Maßnahme darf durch Staatsanwälte angeordnet werden, die in Verbindung mit den Nachrichtendiensten stehen, so z.B. durch den Staatsanwalt, der zum EYP abgeordnet ist. Denn wie schon erwähnt, sind die Informationen der Nachrichtendienste „Vorfeldkenntnisse" und die Ermittlungsschwellen liegen unter den hohen Anforderungen der grStPO. Die Prüfung der formellen und materiellen Rechtmäßigkeit der nachrichtendienstlichen Telekommunikationsüberwachung durch eine unbefangene externe Instanz ist somit erforderlich, bevor die dadurch erhobenen Informationen als Beweismaterial im Strafprozess verwendet werden dürfen.

b) Zulässigkeit der Vernehmung des Nachrichtendienstpersonals als Zeugen

Nachrichtendienstliche Informationen können auch durch einen Zeugenbeweis ins Strafverfahren eingeführt werden. In diesem Zusammenhang stellt sich die Frage, ob die Beamten der Nachrichtendienste als Zeugen in einem Gerichtsprozess aussagen dürfen. Gem. Art. 210 Fall a) grStPO dürfen die Personen, die Ermittlungs- oder staatsanwaltschaftliche Aufgaben in dem betroffenen Fall ausgeübt haben, als Zeugen nicht vernommen werden.[62] Gem. Art. 212 § 1 Fall β) grStPO dürfen Beamte nicht vernommen werden, wenn es sich um militärische oder diplomatische Geheimnisse oder um Geheimnisse bezüglich der Staatssicherheit handelt. Sie dürfen allerdings dann als Zeugen aussagen, wenn der zuständige Minister dies genehmigt. Die Beamten der DIDAP und der Hellenic FIU dürfen somit nur dann nicht als Zeugen aussagen, wenn es sich um ein Staatsgeheimnis diplomatischer oder militärischer Natur handelt. Dies ist allerdings gerade bei der Hellenic FIU nicht der Fall, denn diese ist für Geldwäsche und Terrorismusfinanzierung zuständig. Für die Beamten und das Personal der EYP gilt gem. Art. 14 § 4 G. 3649/2008 i.V.m. Art. 5 § 5 PVO 81/2019 ein Aussageverbot, es sei denn, die Vernehmung wird durch den Premierminister genehmigt. Art. 218 grStPO sieht besondere Maßnahmen zum Schutz der Zeugen im Ermittlungs- und Strafverfahren wegen bestimmter Kriminalitätsbereiche (z.B. Terrorismus, organisierte Kriminalität, Menschenhandel) vor. Beamte der

---

[62] Ausführlich zu den Problemen in *Pavlou*, PoinChron. 2015, 161, 165–166, m.w.N.

Nachrichtendienste sind im Gesetz nicht ausdrücklich genannt. Vom Wortlaut ist aber nicht auszuschließen, dass auch ihnen dieser Schutz gewährleistet werden kann. Derartige Schutzmaßnahmen bestehen in der Anonymisierung, in der Vernehmung mittels visuell-akustischer oder nur akustischer technischer Mittel sowie in der Versetzung oder Abordnung des Zeugen auf unbestimmte Zeit.

2. Beweisverbote in der grStPO und dem grGG

Für die Strafverfolgungsbehörden gelten die Normen der grStPO über die Beweiserhebung bzw. die Beweisverwertung vor einem Strafgericht. Auch ist die Informationsbeschaffung durch das grGG (Art. 9, 9A, 19 grGG zur Privatsphäre, Kommunikation und Datenschutz, Art. 7 § 2 grGG zum Folterverbot, Gesundheits- und Körperverletzungsverbote, etc.) sowie durch einfache Gesetze, z.B. Art. 370 ff grStGB zum Schutz von Geheimnissen und der Privatsphäre im Schriftverkehr und bei der Telekommunikation, beschränkt.[63] Sollte eine polizeiliche Ermittlungsmaßnahme durch einen Nachrichtendienst durchgeführt werden, dann ist zu prüfen, ob die Ermittlung als Eingriff in die subjektiven Rechte des Betroffenen auf einer gesetzlichen Grundlage, der sog. Ermächtigungsgrundlage, beruht und ob sie die Voraussetzungen dieser Grundlage erfüllt.

Im griechischen Strafprozessrecht gilt der Grundsatz der freien Beweiswürdigung. Art. 177 § 1 grStPO sieht vor, dass der Strafrichter nicht an Beweisregeln gebunden ist. Er darf den Sachverhalt nach seiner Überzeugung und seinem Gewissen unbefangen beurteilen. Das Strafgericht darf somit jedes Beweismittel würdigen und akzeptieren. Seine Entscheidung muss es aber begründen. In der grStPO sind einige Beweiserhebungs- und -verwertungsverbote geregelt. Die allgemeine Rechtsnorm für die Beweisverbote gem. Art. 177 § 2 grStPO lautet: „Beweismittel, die durch Straftaten oder mittels Straftaten erhoben wurden, bleiben im Strafprozess unberücksichtigt“. Der Strafprozess im Sinne des Artikels umfasst alle Stadien vom Ermittlungs- bis zum Gerichtsverfahren. Eine ausdrückliche Regelung über die strafprozessuale Konsequenz der Verletzung des Beweisverwertungsverbots ist nicht vorhanden. Jedoch gilt, soweit die Verwertung von illegalen Beweismitteln im Gerichtsprozess die Verteidigungsrechte des Angeklagten verletzt, führt diese Beweisverbotsverletzung zur absoluten Unwirksamkeit des Verfahrens, des Gerichtsurteils und der Ermittlungsmaßnahmen, gem. Art. 171 § 1 Fall δ) grStPO und stellt einen Revisionsgrund gem. Art. 510 § 1 Fall A) grStPO dar.[64]

Eine Beweisverbotsnorm ergibt sich auch aus der griechischen Verfassung. Art. 19 § 3 grGG sieht vor, dass die Verwertung von Beweismitteln verboten ist, die durch einen Verstoß gegen Art. 19 grGG (Geheimnis des Schriftverkehrs und der

---

[63] In Deutschland lässt sich ein Beweisverwertungsverbot auch aus dem Trennungsgebot ableiten, vgl. *Gusy*, ZRP 1987, 45, 51.

[64] Vgl. *Karras*, grStPO Art. 177, S. 360; *Androulakis*, Grundbegriffe, S. 456, Rn. 774a.

Freiheit der Kommunikation), gegen Art. 9 grGG (Schutz der Unverletzlichkeit der Wohnung, des Privat- und Familienlebens) sowie gegen Art. 9A grGG (Schutz der personenbezogenen Daten) erhoben worden sind. Diese Norm wird teleologisch insoweit erweitert, als das Verwertungsverbot auch für andere Grundrechtsverletzungen (z. B. Verletzung der Menschenwürde gem. Art. 2 § 1 grGG bei Beweiserhebung unter Anwendung von Folter) gilt.

Trotz des absoluten verfassungsrechtlichen Verbots in Bezug auf Beweismittel gem. Art. 19 § 2 grGG, trotz des allgemeinen Erhebungs- und Verwertungsverbots bei der Erlangung durch Straftaten wird sowohl im griechischen Schrifttum wie auch in der griechischen Rechtsprechung vertreten, dass diese Verbote nicht absolut gelten. Zum einen ist fraglich, ob das Beweisverbot ausschließlich Beweismittel betrifft, die – gem. dem Wortlaut des Art. 177 § 2 grStPO – durch „*strafbare* (αξιόποινες) Taten" erhoben worden sind, oder auch solche, die durch sonst rechtswidrige Taten erlangt wurden.[65] Zum anderen wird problematisiert, was passiert, wenn ein Beweismittel durch eine rechtswidrige Tat erhoben wird und die Norm zwar die Erhebung dieses Beweismittels verbietet, aber nicht zusätzlich bestimmt, ob dieses Beweismittel dennoch im Gerichtsprozess verwendet werden darf.[66] In solchen Fällen ist die Verwertbarkeit des rechtswidrig (aber nicht strafbar) erhobenen Beweismittels das Ergebnis einer Abwägung von Gründen und Interessen durch den Richter.[67] Die Abwägungslehre wird zudem im Rahmen der Prüfung der Verwertbarkeit des auch strafbar erhobenen Beweismittels angewendet. So gilt das Verbot des Art. 177 § 2 grStPO nicht, wenn das illegale Beweismittel das einzige geeignete Mittel zum Beweis der Unschuld des Angeklagten ist[68] oder wenn das Beweismittel das einzige geeignete und verhältnismäßige Mittel zum Schutz des Opfers durch die Strafrechtsordnung ist, was bedeutet, dass es auch zu Lasten des Angeklagten angewendet werden darf.[69] Einheitlich wird aber angenommen, dass der absolute Charakter des Beweisverbots gilt, wenn das Beweismittel durch Folter oder andere schwere Verletzungen der Menschenwürde erhoben wurde.[70] Dann darf keine Abwägung unter der Anwendung des Verhältnismäßigkeitsgrundsatzes stattfinden.

---

[65] Nach einer Ansicht lässt sich die Norm aber auch so auslegen, dass eine Tat genügt, die die Rechte des Angeklagten verletzt bzw. eine rechtswidrige Tat ist, die nicht unbedingt auch strafbar sein muss, so *Margaritis*, grStPO Art. 177 Rn. 30.

[66] Zur Problematik *Karras*, grStPO Art. 177, S. 361–364.

[67] Dazu *Margaritis*, grStPO Art. 177 Rn. 26–29; *Androulakis*, Grundbegriffe, S. 210 Rn. 317.

[68] Vgl. *Androulakis*, Grundbegriffe, S. 211 Rn. 320; *Karras*, grStPO Art. 177 S. 363; Margaritis, grStPO Art. 177 Rn. 26.

[69] Vgl. *Margaritis*, grStPO Art. 177 Rn. 28. Skeptisch gegenüber der Abwägungslehre und dem Verhältnismäßigkeitsgrundsatz zu Lasten des Angeklagten *Karras*, grStPO Art. 177 S. 361–362.

[70] Vgl. u.a. *Androulakis*, Grundbegriffe, S. 210 Rn. 317–318; *Margaritis*, grStPO Art. 177 Rn. 27.

3. Gerichtliche Praxis hinsichtlich nachrichtendienstlicher Informationen

Aus der gerichtlichen Praxis lassen sich einige Erkenntnisse darüber gewinnen, wie die Gerichte nachrichtendienstliche Informationen als Informationsquellen behandeln. Die Ausführungen beschränken sich auf wenige Fallbeispiele aus der höchstrichterlichen Rechtsprechung des Areios Pagos (Άρειος Πάγος, AP) und des sog. Hellenischen Staatsrates (Συμβούλιο της Επικρατείας, StE).[71] In einem Fall[72] ging es um eine Manipulation von Treibstoffen durch ein griechisches Unternehmen. Die Zollbehörden erhielten Informationen über dieses Unternehmen durch den EYP, Privatpersonen und das Finanzministerium. Das Gericht befasste sich mit der Art der Informationsermittlung nicht. Interessant an diesem Fall ist auch, dass der Fall den Zeitraum von 1993 bis 1994 betraf. Damals war noch das G. 1645/1986 gültig. Laut dessen Art. 2 gehörten Verstöße gegen Zollgesetze nicht zum Tätigkeitsbereich des EYP. Auch Aufträge, die ihm durch den Premierminister hätten gegeben werden können, hätten eine Relevanz zu den Tätigkeitsbereichen des EYP hinsichtlich der Spionage und der nationalen Sicherheiten haben müssen, so der Wortlaut des Art. 2 § 1 Fall δ G. 1645/1986 über „συναφής", d.h. relevant.

In einem weiteren Fall[73] wurde über die Disziplinarstrafe der Entlassung eines Angestellten des EYP entschieden, der in der griechischen Botschaft in Islamabad tätig war und Visa gegen Entgelt ausstellte, ohne dass die gesetzlichen Voraussetzungen dafür erfüllt waren. In diesem Fall ging es um eine internationale Zusammenarbeit zwischen dem EYP, deutschen, französischen und pakistanischen Behörden. Die Informationen stammten von den pakistanischen Behörden und der EYP wurde durch das BKA über den Fall informiert. Zum Zeitpunkt der Entlassung befand sich der Strafprozess gegen ihn nur im Stadium der Anklageerhebung wegen Urkundenfälschung und Bestechung im Amt. Der EYP wurde aufgrund eines Auftrags des Außenministers tätig. Mit der Frage, wie die Informationen gegen diese Person erhoben wurden, befassten sich die Gerichte wiederum nicht.

In einem anderen Korruptionsfall ließ der Areios Pagos (AP)[74] Telefongespräche und Nachrichten als Beweismittel zu, die durch die Telekommunikationsüberwachung seitens des EYP legal und auf der Grundlage eines Justizbeschlusses aufgezeichnet worden waren. Eine Prüfung der Rechtmäßigkeit dieses Beschlusses wie auch der besonderen Umständen der Überwachung nahm das Gericht nicht vor. Zu erwähnen ist auch ein jüngerer Fall von Steuerhinterziehung. In seiner Entscheidung nahm der AP[75] an, dass der Angeklagte falsche Angaben hinsichtlich seines

---

[71] Das sog. Συμβούλειο της Επικρατείας (Regionsrat, StE) ist das höchste Gericht in Griechenland für verfassungs- und verwaltungsrechtliche Angelegenheiten. Es entspricht dem deutschen BVerfG und BVerwG.

[72] StE 1326/2013, veröffentlicht in www.adjustice.gr.

[73] StE 2406/2000, www.adjustice.gr.

[74] AP 804/2019, veröffentlicht in www.areiospagos.gr, zuletzt besucht am 20.12.2019.

[75] AP 528/2019, veröffentlicht in www.areiospagos.gr, zuletzt besucht am 20.12.2019.

Bankkontos in seiner Steuererklärung gemacht hat. Als Beweismittel für die tatsächlichen Kontodaten ließen die Gerichte die Ergebnisse einer Untersuchung der Hellenic FIU zu.

Aus dieser kurz dargestellten Rechtsprechung ergibt sich, dass die Gerichte von Amts wegen eine Prüfung der Rechtmäßigkeit der Erhebung von nachrichtendienstlichen Informationen nicht vornehmen. Auch scheint es nicht problematisch zu sein, diese Informationen als Beweismittel im Hauptverfahren zuzulassen, zumindest solange die Rechtswidrigkeit der Erhebung nicht offensichtlich ist oder diese von dem Angeklagten nicht in Frage gestellt wird.

Zusammenfassung und Würdigung

Zusammenfassend lässt sich feststellen, dass in Griechenland drei Behörden existieren, die sich mit der Informationssammlung, -analyse und -verwaltung befassen und deswegen als Nachrichtendiente zu qualifizieren sind: Der Nationale Informationsdienst (EYP), die Direktion für die Verwaltung und Analyse von Informationen der Hellenischen Polizei (DiDAP) und die Hellenic Financial Intelligence Unit (Hellenic FIU). Im ersten Teil wurde die Frage untersucht, ob und wie weit diese Dienste für die Verbrechensbekämpfung operationalisiert werden. Alle drei Behörden weisen organisatorische Besonderheiten auf, die sie in die Nähe der Strafverfolgung rücken lassen, und ihre Einordnung in der Sicherheitsarchitektur des griechischen Staates ist aus diesem Grund nicht unproblematisch. Der EYP als Inlands- und Auslandsdienst des griechischen Staates ist direkt dem Premierminister untergeordnet. Die DiDAP ist der selbstständige Nachrichtendienst der Polizei. Die Hellenic FIU ist eine Art Mischbehörde. Sie ist zum einen eng mit dem Finanzsektor des Staates verbunden, zum anderen wird sie im Bereich der Wirtschaftskriminalität insbesondere der Geldwäsche und der Steuerhinterziehung sowie des Terrorismus und der Terrorismusfinanzierung mit der Informationssammlung und dem Vollzug von Strafen tätig. Des Weiteren erfüllt sie eine finanzamtliche Funktion hinsichtlich der Aufnahme der Vermögenssteuerklärungen von Personen. Die Ermittlungsschwelle bei allen drei Diensten ist niedriger als bei einem Anfangsverdacht im Sinne der grStPO. Hinsichtlich ihrer Aufklärungsfelder ergeben sich Überschneidungen, da alle drei Dienste mindestens bei den Bereichen Terrorismus, Terrorismusfinanzierung, Geldwäsche und Cyberkriminalität tätig werden. Eine funktionale Aufteilung zwischen den Diensten und den Strafverfolgungsbehörden ist zunächst zwar festzustellen, allerdings ist die Tendenz zur Erweiterung ihrer Befugnisse sowie eine Vernachrichtendienstlichung der Polizei durch die DiDAP festzustellen, so dass die Nachrichtendienste mindestens mittelbar auch für die Verbrechensbekämpfung vor allem im Rahmen der Prävention operationalisiert werden.

Es stellt sich die Frage, wie die Interaktion zwischen den Nachrichtendiensten und den Strafverfolgungsbehörden zu bewerten ist. Dies lässt sich aus dem Blickwinkel des Trennungsgebots, wie es in Deutschland existiert, rechtsvergleichend gut untersuchen. Die funktionale Trennung zwischen den Nachrichtendiensten und den Strafverfolgungsbehörden ist schwach, was sich vor allem an der Vernachrichtendienstlichung der Polizei durch die DiDAP zeigt. Eine organisatorische Trennung ist zwar anhand von formalen Kriterien erkennbar, aber die personelle Trennung wird durch den Personalaustausch zwischen Nachrichtendiensten, Polizei, Strafverfolgungsbehörden und Justiz mittels Abordnung bzw. Versetzung abgeschwächt. Eine informationelle Trennung ist zwar in dem Sinne vorhanden, dass jeder Nachrichtendienst Informationen zur Erfüllung der eigenen Aufgaben sammelt, allerdings verfügt das griechische Regelwerk nicht über detaillierte Rechtsnormen, die diese Trennung bzw. die informationelle Zusammenarbeit der Nachrichtendienste und der Strafverfolgungsbehörden regeln. Die Rechtsnormen über die informationelle Zusammenarbeit stellen Generalklauseln dar, die als Ermächtigungsgrundlage für den Antrag und die Zulässigkeit der Übermittlung und als Grundlagen für die Begründung von Übermittlungspflichten dienen. Beschränkungen der Informationsübermittlung ergeben sich grundsätzlich durch Regelungen über die Geheimhaltungspflichten, die der Speicherung der Informationen zeitliche Grenzen ziehen oder Rechte der Nachrichtendienste, aus besonderen Gründen die Übermittlung von Informationen abzulehnen. Hinsichtlich der strafprozessualen Zulässigkeit von nachrichtendienstlichen Informationen gibt es besondere Rechtsnormen nur in Bezug auf das Beweismaterial, das aus der Telekommunikationsüberwachung stammt. Einzelne Einschränkungen ergeben sich aus der grStPO hinsichtlich der Möglichkeit der Vernehmung nachrichtendienstlichen Personals als Zeugen. Das griechische Strafprozessrecht enthält zwar strenge Regelungen über die Beweiserhebung und Beweisverbote. Diese Strenge wird aber durch die Anwendung des Verhältnismäßigkeitsgrundsatzes abgeschwächt. Das griechische Strafprozessrecht befasst sich im Ergebnis mit dem Phänomen der nachrichtendienstlichen Informationen nicht ausdrücklich.

Insgesamt ist festzuhalten, dass in Griechenland keine strenge Trennung zwischen den Nachrichtendiensten und den Strafverfolgungsbehörden besteht. Dies ist wohl keine nationale Besonderheit, sondern geschieht im Rahmen der internationalen Entwicklung eines immer weiter ausgedehnten Sicherheitsrechts als Reaktion auf die Risiken der digital vernetzten Gesellschaft. Die Information erweist sich als zentraler Machtfaktor und die Herrschaft darüber ist Voraussetzung für die effektive Prävention und Bekämpfung dieser Risiken. Das Zusammenrücken der Sicherheitsbehörden ist wohl auch Folge einer zweidimensionalen Natur von neuen Kriminalitätsphänomenen. Ein Cyberangriff wie auch ein terroristischer Angriff kann nicht mehr klar als eine politische, kriegerische oder eine lediglich strafrechtlich relevante Handlung qualifiziert werden. Er kann sowohl die innere Sicherheit eines Staates wie auch die äußere Sicherheit und die Beziehungen zu anderen Staates beeinträchtigen. Auch kann er die demokratische Verfassungsordnung beeinträchtigen. Zu

denken ist z.B. an die Erklärung des staatlichen Notstands und die damit einhergehende Einschränkung von Grundfreiheiten der Bürger als Folge eines terroristischen Attentats. Die Notwendigkeit eines Nachrichtendienstes im Bereich der äußeren Sicherheit eines Staates im Rahmen des Schutzes der Diplomatie, der Spionage-Bekämpfung und der Verteidigung der Demokratie liegt auf der Hand. Eine Notwendigkeit z.B. im Bereich des Terrorismus gleich drei Nachrichtendienste tätig werden zu lassen, kann aber so nicht begründet werden.

Als der Exekutive nahstehende Organe muss die Tätigkeit von den Nachrichtendiensten auch legitim und legitimiert sein und an die gleichen Grundsätze und Rechtsgarantien gebunden sein, die auch für die Exekutive gelten. Aspekte der legitimen Tätigkeit der Nachrichtendienste[76], die bei einer Reform des griechischen Nachrichtendienstrechts berücksichtigt werden müssen, sind die hinreichende Bestimmung ihrer Aufgaben und der Befugnisnormen ihres Modus Operandi, die hinreichende Bestimmung der Ermittlungsschwelle und der Voraussetzungen ihres Eingriffs in die subjektiven Rechte der Bürger und die Gewährleistung von Kontroll- und Aufsichtsmechanismen für ihre Tätigkeit.

Ein wichtiger Grundsatz für die Struktur und Tätigkeit der Nachrichtendienste ist auch das Trennungsgebot. Zwar ist dieses in der griechischen Jurisprudenz nicht bekannt; da der griechische Staat aber auch eine demokratische, freiheitliche rechtstaatliche Ordnung hat und der Schutz der informationellen Selbstbestimmung, der Privatheit und der Kommunikation garantiert sind, ist die rechtstheoretische Grundlage für die Herausarbeitung eines Trennungsgebots in Griechenland als Leitgrundsatz für die Umstrukturierung und Gestaltung der Nachrichtendienste vorhanden.

Die Sicherheitsarchitektur einschließlich der Nachrichtendienste sowie deren Tätigkeit im Bereich der Verbrechensbekämpfung sollte so gestaltet werden, dass diese Trennung gewährleistet wird. Die Unabhängigkeit und Unbefangenheit der Nachrichtendienste sollte durch die Unabhängigkeit des Personals garantiert werden, indem der Personalaustausch eingeschränkt wird.[77] Die Abordnung von Staatsanwälten zu den Nachrichtendiensten, die entweder die Behörde führen, z.B. wie bei der Hellenic FIU oder die Rechtmäßigkeit ihrer Tätigkeit kontrollieren, z.B. bei der DiDAP und dem EYP, stellt sicherlich ein Zeichen für die Bedeutung der Rechtmäßigkeit und Legitimität ihrer Praxis dar. Aufgrund dessen, dass die Staatsanwälte aber dorthin abgeordnet werden, könnten Bedenken bezüglich ihrer Unbefangenheit begründet werden, z.B. wenn die gleiche Person den Nachrichtendienst führt und zugleich ihre Tätigkeit genehmigen und beaufsichtigen soll. Die Tätigkeit der Nachrichtendienste im Bereich der operativen Verbrechensbekämpfung sollte ein-

---

[76] Vgl. ähnlich *Dervitsiotis*, in: Staat – Sicherheit, 105, 109.

[77] Zumal oft der Personalaustausch Gegenstand von „Kleinklientelpolitk" zwischen Ministern und Sicherheitsbehörden ist, was auch die Effektivität der Nachrichtendienste beeinträchtigen kann, vgl. dazu *Apostolidis*, EYP, 23–24. Ähnlich auch *Alivizatos*, NoB 1983, 621, 630.

geschränkt nur für ihre Zwecke erfolgen, z.B. für die Entwicklung einer nationalen Sicherheitspolitik. Kontrollmechanismen sollten verstärkt werden. Insbesondere für den EYP sollte die lange ausgebliebene Reform der parlamentarischen Geschäftsordnung nachgeholt werden und auch er unter parlamentarische Kontrolle gestellt werden.

Informationsübermittlungspflichten in der Form von Generalklauseln oder unbestimmten Ermächtigungsgrundlagen sind in Zeiten der technischen Möglichkeiten des Datenabgleichs und der Datenverknüpfung nicht ohne Einschränkungen einzuführen. Die Informationsübermittlung darf nicht nur im freien Ermessen des Nachrichtendienstes stehen. Informationsübermittlungsregelungen verstoßen dann nicht gegen das Trennungsgebot, wenn sie z.B. zu keiner gemeinsam geführten und uneingeschränkt abrufbaren Datenbank von gespeicherten Informationen führen, die allen Behörden durch eine direkte ungehinderte Verbindung verfügbar wären. Im Rahmen des Polizeirechts sind Regelungen der Amtshilfe vorhergesehen, die auch die informationelle Zusammenarbeit zwischen Behörden regeln. Zu klären ist, in welchem Verhältnis diese Normen zu den oben genannten Informationsübermittlungspflichten stehen und ob und wie die Institution der Amtshilfe dadurch verändert wird.

Zuletzt ist zu überlegen, wie das Ermittlungsverfahren durch die Nachrichtendienste strafprozessual zu qualifizieren ist. Davon ist auch abhängig, welche Verteidigungs- und Schutzrechte für die von den Ermittlungen Betroffenen zu gewährleisten sind. Während des Untersuchungsverfahrens im Sinne der grStPO wird noch keine Anklage erhoben, deswegen hat der Betroffene nicht den vollständigen Rechtsstatus des Angeklagten. Die betroffene Person ist nur ein Verdächtiger, damit sind ihr weniger Rechte als einem Angeklagten eingeräumt, Art. 244 grStPO. Dazu gehört auch das Recht auf Gehör innerhalb von 48 Stunden. Die Person wird durch die Staatsanwaltschaft innerhalb einer gesetzlich bestimmten Frist ab Beginn des Untersuchungsverfahrens eingeladen, um sich über den zu untersuchenden Sachverhalt zu äußern. Entsprechende Ermittlungen durch die Nachrichtendienste sind lange nach dem Grundsatz der Geheimhaltung nicht öffentlich und ein Recht der Person auf Benachrichtigung, dass wegen Straftaten Informationen über sie gesammelt werden, ist nicht vorgesehen. Zu überlegen ist also, ob diese Ermittlungen als „Quasi-Untersuchungen im strafprozessualen Sinne“ zu qualifizieren sind und wie dadurch die strafprozessuale Position der betroffenen Person gestärkt werden kann.

Literaturverzeichnis

Alivizatos, Nikos K.: Der Rechtsstatus der Sicherheitskörperschaften, in: Nomiko Vima 1983, S. 621–633 (auf Griechisch: Αλιβιζάτος, Νίκος Κ.: Το νομικό καθεστώς των σωμάτων ασφαλείας, σε: Νομικό Βήμα 1983, σελ. 621–633). (Zit.: *Alivizatos*, NoB 1983, 621, …).

Androulakis, Nikolaos K.: Grundbegriffe des Strafprozesses, Athen 4. Auflage 2012 (Auf Griechisch: Ανδρουλάκης, Νικόλαος Κ.: Θεμελιώδεις Έννοιες της Ποινικής Δίκης, Αθήνα 4. Έκδοση 2012). (Zit.: *Androulakis*, Grundbegriffe, S. … Rn. …).

Apostolidis, Pavlos: Die Informationsdienste im nationalen Sicherheitssystem – Der Fall von EYP, Athen 2007 (auf Griechisch: Αποστολίδης, Παύλος: Οι Υπηρεσίες Πληροφοριών στο Εθνικό Σύστημα Ασφαλείας: Η περίπτωση της ΕΥΠ, Αθήνα 2007). (Zit.: *Apostolidis*, EYP, S. …).

Dagtoglou, Prodromos D.: Verfassungsrecht – Grundrechte, 3. Auflage 2010, Athen – Komotini. (Auf Griechisch: Δαγτόγλου, Πρόδρομος Δ.: Συνταγματικό Δίκαιο – Ατομικά Δικαιώματα, 3. έκδοση 2010, Αθήνα – Κομοτηνή). (Zit.: *Dagtoglou*, Grundrechte, S. … Rn. …).

Dervitsiotis, Alkis: Auf der Suche nach der (schwierigen) Legitimation der Nachrichtendienste – Aspekte der europäischen Erfahrung, in: Staat-Sicherheit und die Rolle der Nachrichtendienste – Der Fall Griechenland – Kompetenzen und Funktion der Nationalen Informationsdienst, Tagungsberichte, Athen 2009, S. 105–112. (Auf Griechisch: Δερβιτσιώτης, Άλκης: Αναζητώντας τη (δύσκολη) νομιμοποίηση των Υπηρεσιών Πληροφοριών – Όψεις της ευρωπαϊκής εμπειρίας, σε: Κράτος – Ασφάλεια και ο ρόλος των υπηρεσιών πληροφοριών – Η περίπτωση της Ελλάδας – Αρμοδιότητες και Λειτουργία της Εθνικής Υπηρεσίας Πληροφοριών, σε Πρακτικά Επιστημονικής Ημερίδας, σελ. 105–112), (Zit.: *Dervitsiotis*, in: Staat – Sicherheit, 105, …)

Dimopoulos, Charalampos: Polizeirecht, Athen 2007 (auf Griechisch: Δημόπουλος, Χαράλαμπος: Αστυνομικό Δίκαιο, Αθήνα 2007). (Zit.: *Dimopoulos*, Polizeirecht, S. …).

Gärditz, Klaus: Anmerkung zum BVerfG Urteil vom 24.4.2013 – 1 BvR 1215/07, in: JZ 2013, S. 633–636. (Zit.: *Gärditz*, JZ 2013, 633, …).

Gusy,Christoph: Das verfassungsrechtliche Gebot der Trennung von Polizei und Nachrichtendiensten, in: ZRP 1987, S. 45–52. (Zit.: *Gusy*, ZRP 1987, 45, …).

Karras, Argyrios: Strafprozessordnung – Systematische Auslegung und Methodische Darlegung pro Artikel, 3. Auflage 2016, Athen. (Zit.: *Karras*, grStPO Art. … S. …).

Kutscha, Martin: Die Aktualität des Trennungsgebots für Polizei und Verfassung, in: ZRP 1986, S. 194–198. (Zit.: *Kutscha*, ZRP 1986, 194, …).

Margaritis, Lampros: Strafprozessordnung – Auslegung pro Artikel, 2. Auflage 2018, Athen – Thessaloniki (auf Griechisch: Μαργαρίτης, Λάμπρος, Κώδικας ποινικής δικονομίας – Ερμηνεία κατ' άρθρο, 2η Έκδοση 2018, Αθήνα Θεσσαλονίκη) (Zit.: *Margaritis*, grStPO Art. … Rn. …).

Mazis, Ioannis: Nationaler Sicherheitsrat, in: Staat-Sicherheit und die Rolle der Nachrichtendienste – Der Fall Griechenland – Kompetenzen und Funktion der Nationalen Informationsdienst, Tagungsberichte, Athen 2009, S. 155–162. (Auf Griechisch: Μάζης, Ιωάννης: Εθνικό Συμβούλιο Ασφάλειας, σε: Κράτος – Ασφάλεια και ο ρόλος των υπηρεσιών πληροφοριών – Η περίπτωση της Ελλάδας – Αρμοδιότητες και Λειτουργία της Εθνικής Υπηρεσίας Πληροφοριών, σε Πρακτικά Επιστημονικής Ημερίδας, σελ. 155–162), (Zit.: *Mazis*, in: Staat – Sicherheit, 152, …).

Nehm, Kay: Das nachrichtendienstliche Trennungsgebot und die neue Sicherheitsarchitektur, in: NJW 2004, S. 3289–3295. (Zit.: *Nehm*, NJW 2004, 3289, …).

Ntokos, Thanos: Die Rolle der Nachrichtendienste im neuen internationalen Sicherheitsumfeld, in: Staat-Sicherheit und die Rolle der Nachrichtendienste – Der Fall Griechenland – Kompetenzen und Funktion der Nationalen Informationsdienst, Tagungsberichte, Athen 2009, S. 65–73. (Auf Griechisch: Ντόκος, Θάνος: Ο ρόλος των υπηρεσιών πληροφοριών στο νέο διεθνές περιβάλλον ασφάλειας, σε: Κράτος – Ασφάλεια και ο ρόλος των υπηρεσιών πληροφοριών – Η περίπτωση της Ελλάδας – Αρμοδιότητες και Λειτουργία της Εθνικής Υπηρεσίας Πληροφοριών, σε Πρακτικά Επιστημονικής Ημερίδας, σελ. 65–73), (Zit.: *Ntokos*, in: Staat – Sicherheit, 65, …).

Papaioannou, Zoi: Inhalt und Grenzen der Polizeigewalt – Die funktionale Kompetenz des Polizeipersonals der Hellenischen Polizei, Athen u.a. 2004 (auf Griechisch: *Παπαϊωάννου, Ζωή*: Περιεχόμενο και όρια της Αστυνομικής Εξουσίας – Η λειτουργική αρμοδιότητα του αστυνομικού προσωπικού της ελληνικής αστυνομίας, Σάκκουλας Αθήνα κ.α. 2004). (Zit.: *Papaioannou*, Polizeigewalt, S. …).

Pavlou, Stefanos.: Die Tonaufnahme von Telefongesprächen verdächtiger Personen durch die Behörden – Institutioneller Rahmen, rechtsstaatliche Grenzen, praktische Verdrehung und Abweichung – Eine erste Darstellung von Problemen und Gedanken, in: Poinika Chronika 2015, S. 161–166. (Auf Griechisch: Παύλου, Στέφανος Κλ.: Η μαγνητοφώνηση τηλεφωνικών συνδιαλέξεων υπόπτων από τις αρχές – Θεσμικό πλαίσιο, δικαιοκρατικά όρια, πρακτικές στρεβλώσεις και εκτροπές – Μια πρώτη καταγραφή προβλημάτων και σκέψεων, σε: Ποινικά Χρονικά ΞΕ (2015), Σελ. 161–166). (Zit.: *Pavlou*, PoinChron 2015, 161, …).

Tachos, Anastasios: Recht der öffentlichen Ordnung, Thessaloniki, 1990 – Auf Griechisch: *Τάχος*, *Αναστάσιος Ι*.: Δίκαιο της Δημόσιας Τάξης, Θεσσαλονίκη 1990). (Zit.: *Tachos*, öffentliche Ordnung, S. …).

Zöllner, Mark A.: Der Rechtsrahmen der Nachrichtendienste bei der „Bekämpfung" des internationalen Terrorismus, in: JZ 2007, S. 763–771. (Zit.: *Zöllner*, JZ 2007, 763, …).

Abkürzungsverzeichnis

ADAE	Behörde zum Schutz des Kommunikationsgeheimnisses (Αρχή Διασφάλισης Απορρήτου Επικοινωνιών, Α.Δ.Α.Ε.).
AP	Areios Pagos (Oberster Gerichtshof)
CERT	Computer Emergency Response Team
DiDAP	Direktion für die Verwaltung und Analyse von Informationen (Διεύθυνση Διαχείρισης και Ανάλυσης Πληροφοριών)
EYP	Εθνική Υπηρεσία Πληροφοριών (ΕΥΠ – Nationaler Informationsdienst)
EL.AS.	Ελληνική Αστυνομία (Hellenische Polizei)
FIU	Financial Intelligence Unit.
G. … / …	Gesetz Nummer/Jahr
grGG	Griechisches Grundgesetz
grStGB	Griechisches Strafgesetzbuch

grStPO	Griechische Strafprozessordnung
IA	Information Assurance
IAA	Information Assurance Authority
INFOSEC	Information Secutiry
JZ	Juristenzeitung.
NIS	National Intelligence Service
NJW	Neue Juristen Wochenschrift.
PVO. …/…	Präsidialverordnung (Προεδρικό Διάταγμα, π.δ.) Nummer/ Jahr
PoinChron.	Poinika Chronika (Ποινικά Χρονικά)
StE	Συμβούλιο της Επικρατείας (Griechischer Oberster Verwaltungs- und Verfassungsgericht).
ZRP	Zeitschrift für Rechtspolitik
ΦΕΚ …/…/….	Φύλλο Εφημερίδας της Κυβερνήσεως (Gesetzgebungsblatt der Regierung) Heft/Nr./Veröffentlichungsdatum.

Organised crime and the Dutch intelligence community

Institutions, concepts, and practices

C.W. Hijzen

I. The police against organised crime[1]

Organised crime is all but a recent phenomenon in the Netherlands. Notorious are the criminal gangs called the *Bokkenrijders* (buck riders), which during their robberies tortured and murdered people, terrorising Limburg in the eighteenth century.[2] Dutch politicians, however, never really considered organised crime as an important problem, and so it took the Dutch state a long time to institutionalise and organise countermeasures. Although locally, Dutch police forces did establish criminal intelligence services in order to improve their capacity to counter organised crime from the 1960s onwards – applying techniques such as observation, reconnaissance, and agent handling – and several regional and national initiatives for the improvement of cooperation were taken, it took quite some time before the urgency of the problem was felt. Even in 1985, as the scholar Cyrille Fijnaut pointed out, whenever the Dutch discussed 'the phenomenon of organised crime', people tended to think of 'spectacular examples' such as the 'Italian mafia or American gangsters', and therefore as

[1] The author is very thankful to prof. dr. P.H.A.M. Abels for his input to this paper.

[2] E.g. A. Blok, *De Bokkenrijders, roversbenden en geheime genootschappen in de Landen van Overmaas (1730-1774)* (Amsterdam, 1991).

something distant and foreign.[3] Only in 1986, after a committee had concluded that the Dutch police had 'insufficient knowledge about what went on in criminal milieux', attempts were made nationally to coordinate and improve the gathering of criminal intelligence.[4]

From then on, criminal intelligence units in several police departments started to run large-scale operations against criminal networks. During those operations informers were recruited, usually in facilitating positions, in order to gain insight into the way that criminal networks operate. During one of those operations, run by an interregional criminal investigation department of Noord-Holland and Utrecht, large shipments of drugs were allowed to be delivered under auspices of the police and the Justice Department. The goal was to use the informers to gain access to the leadership of a specific criminal gang, the 'heirs of Bruinsma' (*de erven-Bruinsma*), but allegations of corruption surfaced and the operation was terminated. Two parliamentary inquiries were held; in particular the last one, that of the Van Traa committee, which presented a 5500-page report in February 1996, prompted important changes in Dutch criminal investigation practices; one of the results was that in the police investigation act (*het wetboek van strafvordering*) the 'special criminal investigation techniques' were more extensively and more explicitly regulated.[5]

II. The intelligence and security services

At about the same time as the Van Traa committee's report, the Dutch security service started to investigate the phenomenon of organised crime too, even though they never had done so before. Besides a military intelligence section at the General Staff, the Central Intelligence Service (in Dutch: *Centrale Inlichtingendienst*), which was established in 1919, only studied political extremism in order to inform authorities about the threat of revolution.[6] And although local police forces collected the intelligence on (mostly) radical socialists, anarchists, and other revolutionary parties at the fringes of the political spectrum, criminal matters were not a part of these domestic intelligence practices.[7]

---

[3] C.J.C.F. Fijnaut, 'Voorwoord', in *Justitiële Verkenningen*, nummer 9 (december 1985), 3–5, there 3. Internet: https://www.wodc.nl/binaries/jv8509-volledige-tekst_tcm28-76159.pdf.

[4] E.g. 2.1.1. Ontstaansgeschiedenis CID'en, *Rijksrechercherapport RCID Kennemerland*, Utrecht 1996. Internet: https://www.burojansen.nl/cid/ and https://www.burojansen.nl/cid/h2-1.htm.

[5] Rapport-Van Traa, Inzake opsporing. Enquetecommissie opsporingsmethoden (Den Haag 1996). Internet: https://www.burojansen.nl/traa/e.htm.

[6] E.C. Braat, 'Dutch intelligence and security services', in P.C. Oleson (ed.), *AFIO's Guide to the Study of Intelligence* (2016) 661–670, there 662.

[7] C.W. Hijzen, 'Bewakers van orde, beschermers der democratie. De Centrale Inlichtingendienst en de politieverbindingen in het Interbellum', *Cahiers Politiestudies*, Jaargang 2017-4, nr. 45 135–162.

The Second World War strengthened this functional division between the police and the intelligence community. Because of the experience of the German invasion and occupation, and specifically the activities of the *Sicherheitsdienst* which operated de facto as political police for the Nazi party leadership, intelligence gathering practices in the post-war era were questioned. Because the Dutch government was convinced, however, that it could not do without these in the post-war world in which the Cold War was unfolding, several foreign intelligence services (both civil and military) and a domestic security service, the *Binnenlandse Veiligheidsdienst* (BVD), were established.

All of these, but because of its operational activities 'at home' most notably the domestic security service BVD, were institutionalised as *information gathering bureaus*, explicitly lacking police powers such as criminal investigation, arrest, and detention. The security services worked, as will be shown, under confidential royal decrees which explicitly withheld police powers from them.[8] When in 1950 parliament questioned whether the security service could legitimately exist in the Dutch parliamentary democracy, the minister of the Interior replied that the BVD 'only' informed government; its institutionalisation was an 'administrative-organisational decision'. The BVD was 'no political police', it did not have 'executive powers' and did not resort to 'Gestapo methods', government argued. Like in West Germany, the *Trennungsgebot* was fundamental for the Dutch security establishment.[9]

The wall between the police and Justice Department on the one side, and the security service on the other, has been fortified ever since. When it became public in 1975 that the BVD relied on intelligence bureaus at the local police departments for many of their activities – police inspectors collected intelligence for the BVD, but also for their police commissioners and mayors to help them uphold public order (and act against demonstrations) – it triggered a parliamentary debate.[10] Would the policeman wearing a 'BVD-hat' really resist using his police powers (such as arresting people and searching their houses) if these police powers suited him in the course of his work for the security service? Was that not a 'completely theoretical' distinction, parliament asked, thus bringing the spectre of the Gestapo back into the realm of politics again? On the one hand, if police officers indeed refrained from using any policing powers in their capacity as 'security service helpers', then it would not be a problem. The police intelligence capability would then be strictly separate. On the other hand, if it became impossible to separate the two in practice, then a certain overlap might legitimately exist: the police might come across useful information for the security service in a criminal investigation. If the security service then opened up

---

[8] E.g. Royal Decree on the Intelligence and Security Services no. 51, 8 August 1949. Article 2.2 reads that the Domestic Security Service 'does not possess any executive powers'. Internet: www.stichtingargus.nl/bvd/par/kb1949.pdf.

[9] C.W. Hijzen, *Vijandbeelden. De veiligheidsdiensten en de democratie* (Amsterdam 2016) 119–120, 123.

[10] Hijzen, *Vijandbeelden*, 250.

its own investigation, the means with which the first intelligence was acquired required would be considered as illegitimate, but if they then began a separate investigation, it would be considered legitimate. The point is, that for the outside world these distinctions were unclear, bewildering vague even. They had no way of knowing whether the separation between the security service activities and police activities would be upheld.[11]

A bit warily, therefore, and occasionally clashing because of their different outlooks and interests, the police and the security service intensified their cooperation in the domain of counterterrorism throughout the 1970s. Whereas the Justice Department took the lead (hostage takings, bombings, and other forms of political violence and terrorism were crimes) the security service and the police developed activities in order to prevent terrorist and politically violent acts. The police did so on the basis of criminal law; the security service did so in order to protect the 'democratic order, state security, and other interests of the state'.[12]

III. The security service and international crime: 1992–2000

After the Cold War, according to some because the security service was desperately looking for new work now that communism had disappeared from the stage, the BVD argued that it should investigate international crime as well. In their annual report for 1992, the security service argued that it should build an intelligence position against international crime in the name of 'the protection of administrative integrity'. The argument in the annual report ran as follows:

> The functioning of our legal order depends to a large extent on citizens' acceptance of and voluntary compliance with the rules as the government has made them. The quality of the rules, the way in which government implements and upholds them – and also public administration itself – must therefore be of high quality. Only a government which continually shows that it wants to behave in compliance with the rules and procedures, can demand of its citizens that they do the same. Government performance, reliable and with integrity, exemplified in transparency and careful decision making and legitimate implementation of the rules, is therefore an important condition for the proper functioning of our legal order.
>
> Although the Dutch public government fortunately still enjoys a reputation of integrity, there is a risk that this might change due to a number of social and administrative developments in the last few years. Social arrangements lost their familiarity, norms and values differentiated, public and private interests intertwined as a result of the fact that the government operates in networks and in public private partnerships, the instrument of

---

[11] C.W. Hijzen, *Vijandbeelden. De veiligheidsdiensten en de democratie* (Amsterdam 2016) 250.

[12] C.W. Hijzen en W.J.M. Aerdts, '20. Vóór de aanslag: terrorismebestrijding door inlichtingen- en veiligheidsdiensten, in: Bakker E., Muller E.R., Rosenthal U., Wijk R. de (red.), *Terrorisme. Studies over terrorisme en terrorismebestrijding (Handboeken Veiligheid)* (Alphen a/d Rijn 2018) 521–545, there 526–528.

administrative toleration developed, and particularly organised crime became an important problem – these factors account for the increase in risks for public administration.

The current, serious political and administrative crisis in Italy shows the potential magnitude of administrative corruption, but also how difficult it is to end it once it acquired a position in the political and administrative culture and how fundamental trust between government, political parties, and citizens can be violated as a result of the lack of the will and attention to seriously oppose such an evil.

It is an illusion to think that these kinds of developments only take place in Mediterranean and Latin American cultures. The phenomenon manifests itself in far more countries; fortunately in the Netherlands only incidentally. Awareness in all administrative levels of the way in which the phenomenon can develop, as well as the advancement of a combination of preventive and repressive measures, is are therefore an important policy goal of the minister of the Interior.

It is, above all, the responsibility of the government organisations themselves to prevent and counter this phenomenon. One can read this in the memo 'Organised crime in the Netherlands' of the ministers of the Interior and Justice, which has been sent to parliament in September 1992.

The way in which, and the locus of breaches of integrity of the government apparatus can be expected to take place, are not always foreseeable. Notably, if organised crime strives to develop a structural grip on a particular sector of government, their secret methods will not be easily exposed. If the governmental body involved would want to fulfil its responsibility, it would need to have adequate knowledge of the problem.

Even though the police and the Justice department have possibilities and responsibilities in this domain, the BVD can contribute in the domain of prevention, against the background of the importance attached to the interest of the integrity of public administration and in order to prevent serious damage to the legal order if the phenomenon would become structural. The BVD will focus in particular on the systematic delineation of the sectors of government that run the largest risk in this respect. Currently, only general notions of the problem are available, largely based on the deduction that the loci of government that run the risk of a violation of integrity, are those in which large sums of money go around, where authorisations are granted, or where oversight and control could contain illegal practices.

During the investigation, the BVD and the governmental bodies involved will make a list of situations in which the chance to make large financial gains without too much risk is relatively great. As a result of unclear or complex rules and regulations, of over-the-top administrative tolerance, or of a lack of oversight and control, opportunity structures for abuse can develop, not only for organised crime, but also for people and organisations that are not criminal in themselves. Trafficking in and exploitation of illegal, foreign women for prostitution, as well as the selling of soft drugs and intermediating of illegal, foreign workers, can for example be very profitable.

Those who try to benefit from such opportunity structures, will take an interest in maintaining and expanding those structures, comparable to the way in which continuity and expansion of opportunities to make profit would be part of a normal entrepreneurial strategy. If this proves to be impossible in time without exercising influence on administrators and other civil servants, for example because it requires authorisations and permits, subsidies, or deviance from rules, or simply for the government to turn a blind eye, then all conditions are present for this to actually happen. It might happen incidentally only in the beginning, but in time structural and systematic attempts can be expected.

Apart from making a list of such vulnerable sectors in the domain of prevention, the BVD has also reached out to the police, the Justice department, and a number of Western European counterparts to investigate their experiences with the methods of organised crime. Based on that knowledge, the BVD plans to provide the government bodies involved with

> knowledge of the way in which the governmental apparatus is capable of defending itself against these serious forms of administrative corruption, so that countermeasures can be introduced in the right places. In addition, one needs to know whether these measures have the intended result and whether government is in fact capable of defending itself against corruption attempts. It is, after all, important not to introduce pre-emptive measures only once, but to develop instruments that provide early warning in case of danger. Generally, one can think of consultation procedures and a hotline through which the first rumours of supposed corruptive behaviour can be investigated quickly and correctly, in order to see with whom the lack of action against it can be discussed. Within its responsibilities in the domain of prevention, the BVD will also contribute to the development of such an instrument.[13]

Without a changed legal framework, the BVD thus developed a new policy in the domain of organised crime, explicitly linked to the integrity of public administration. It framed organised crime as a threat to the democratic order and therefore as a phenomenon that it should investigate. What 'the democratic order' exactly was, was not explicitly defined or discussed in the Royal Decrees, nor in the 1987 Act for the Intelligence and Security Services. Throughout the Cold War, its definition always linked to the concept of extremism or 'antidemocratic forces'. Although never formally documented, extremism and antidemocratic forces were understood as those people and organisations who subscribed to an ideology that – in the end – wants to subvert or destroy the democratic order altogether, i.e. communists. They were considered to be politically, socially, economically, and culturally active in order to advance communism. In the end, perhaps only in the distant future, they would have to replace the democratic order with a socialist state. By being a member of communist organisations or a reader of communist outlets, people were in the eyes of the security service seen as subscribers to that ideology, and hence a threat to the democratic order.[14]

In the post-Cold War era, however, the landscape of threats changed markedly. Internally and externally the BVD had to identify new threats to the democratic order, and for – more or less – the first time, the security service more elaborately addressed what the term meant. In the first openly published annual report, the BVD wrote:

> The responsibilities of the BVD in the domain of the democratic order, are aimed at the unimpeded functioning of democratic decision-making processes and the free exercise of constitutional rights. Political decision-making should materialise according to democratic rules and it should be free from secret or violent influence. The activities of the BVD are aimed at warning early about who could exercise such influence and where it presumably would materialise. […] The identification of activities and developments that might lead certain groups in our society to be impeded in the exercise of their constitutional rights, is the second main responsibility.[15]

---

[13] BVD Annual report 1992, 13–15. Internet: http://www.inlichtingendiensten.nl/jaarkwartaalmaand/Jaarverslag_AIVD_1992.pdf

[14] Hijzen, *Vijandbeelden*, passim.

[15] BVD annual report 1992, 8. Internet: http://www.stichtingargus.nl/bvd/jaar1992.pdf.

The security service now argued that cases of fraud, money laundering, and corruption could – in the long run – harm the democratic rule of law. The service started to analyse cases, in order to assess the damage to the system and to help public services to protect themselves against integrity violations. In the 1990s, the security services therefore developed their own method which public services should use for a form of 'self-examination'. From 1996, the BVD played a role in detecting the activities of criminal organisations to hinder and obstruct criminal investigations, as long as it was linked to the (threatened) continued functioning of the democratic order. In this period, the Dutch security service started intelligence operations against criminal organisations and persons for the first time, with a special focus on what was called 'the underworld and the upper world intertwining'. In the end, a citizen would need to be able to trust blindly the civil servant in front of him or her, whether it was a local or a national one. Organised crime infringed upon that trust.[16]

Even though it turned out to be very complicated to run agents in criminal networks for the security service, as the biography of former BVD employee Paul Herrie (a former agent handler who worked against organised crime) shows, the security service continued to consider international crime as one of their objects of attention.[17] After several incidents and failures, the service came to the conclusion that their legal framework and special powers were not suitable for crime fighting. In the annual report for 2000 they rather briefly concluded the following:

> In its research on a number of its foci of study, such as arms trade and illegal migration, the BVD regularly receives signals of criminal offenses being committed. The Public Prosecutor is informed of these acts through an official message. In addition, the BVD investigates aspects that have related to organised crime for a number of years. This involves breaches of integrity and supposed cases of counter strategies that infringe upon the normal processes of investigation and prosecution.
>
> In 2000, these activities relating to organised crime have been evaluated. The evaluation confirmed the position that organised crime in itself should not be a focus of the BVD. The BVD is not involved in investigating criminal offenses. It does have added value on those aspects that might pose a threat to the integrity of the public sector.[18]

And with that, the BVD claimed the exact opposite of what it argued in 1992: that organised crime should *not* be a topic of research. Although this seems to have implied a shift in the threat perception of organised crime and the way that it functions, it could well have been practical considerations that led the BVD to end their activities in this domain. The focus of the security service on crime fighting was now reduced to (a few) cases in which the integrity of public administration was evidently at stake, a situation which still exists today. Strikingly, recently, the Dutch minister

---

[16] E.g. BVD annual report 1998, 13. Internet: http://www.stichtingargus.nl/bvd/jaar1998.pdf.

[17] M. Husken en H. Lensink, *Spion in de onderwereld: opkomst en ondergang van geheim agent Paul H.* (Amsterdam 2011).

[18] BVD annual report 2000, 7.5. Internet: http://www.stichtingargus.nl/bvd/jaar2000.pdf.

of Justice Ferd Grapperhaus announced that he wanted the Dutch intelligence community to fight international drugs criminals abroad. Although he seemed, rather pragmatically, to want to use the special powers of the intelligence and security services abroad – which for the Public Prosecution Office are very limited – he redefined in the process the extent to which organised crime poses a threat to the democratic order.[19]

IV. The legal framework and organisation[20]

Against this background, the police and criminal prosecution, on the one hand, and the intelligence and security services, on the other, were institutionalised in different legal frameworks and organisations. The Public Prosecution Office, the police, and the Justice Department each have their own powers, their own resources, and there are different legal consequences to their actions. The police, for example, work under the Police Law of 2012.[21]

The legal framework of the intelligence and security services is different. From 1946 onwards, the intelligence community was founded on the basis of Royal Decrees. In 1987, the first Act for the Intelligence and Security Services was introduced. It consisted of more or less the same formulations as the Royal Decree of 1972, but in 2002 the Act was vastly expanded. In terms of legality, the *Hoge Raad*, or supreme court, ruled on 9 June 1994 that the activities of the Dutch security service were no longer in line with article 8(2) of the European Convention on Human Rights, which stated that interference with the right to a private life could only occur if it was legally allowed.[22] To meet that criterion, the *Hoge Raad* argued that the Netherlands should more clearly define under what circumstances Dutch citizens could – in the name of national security – be subjected to privacy-infringing activities: when they can reasonably expect to have their phones tapped or emails intercepted, for example. The Act of 2002 was therefore a *codification* of existing collection practices.[23] Because the Act did not allow the intelligence and security services untargeted access to cable-bound telephone and internet traffic, it was updated in 2017. The intelligence

---

19 E.g. *NRC Handelsblad*, 23 September 2019.

20 The author is very grateful to Clotilde Sebag for her help with this section.

21 Internet: https://wetten.overheid.nl/BWBR0031788/2013-05-01.

22 Quoted in the Review Committee for the Intelligence and Security Services report no. 19, 4. The ruling of the Hoge Raad was: Afdeling Bestuursrechtspraak van de Raad van State 9 juni 1994, *AB* 1995/238 (Van Baggum).

23 R. Dielemans, 'De Wiv 2002 en Wiv 2017 op enkele hoofdlijnen vergeleken', *Justitiële Verkenningen*, 2018, nr. 1, 68–84. Internet: https://www.wodc.nl/binaries/JV1801_Volledige%20tekst_tcm28-309179.pdf#page=69.

community argues that they need this access, because this provides them with metadata which can be used for contact-chaining and mapping networks of targets.[24]

These special powers can only be used when they meet specific criteria. The security services have to ask the minister of the Interior whether they can use their powers to tap someone's phone or hack into a computer, for example. If the minister grants them authorisation, the power can be applied only for a limited period of time – every tap, hack, or agent operation has to be evaluated after a few months in order for it to be prolonged. In order to oversee all this, two independent oversight committees – one ex ante and one ex post – review whether the application of this specific special power in each specific case was indeed necessary (national security is at stake), proportionate (applying the infringing special power is proportionate in the sense that the threat, if materialised, would pose grave harm to national security), and subsidiary (it is impossible to collect the intelligence in another way).

The Act for the Intelligence and Security Services (*Wet op de Inlichtingen- en Veiligheidsdiensten* or WIV), called here the ISS Act 2017, statutorily defines the tasks and powers of the intelligence security services. In the Act for the Intelligence and Security Services it defines that there are two services that combine intelligence and security – the General Intelligence and Security Service (*Algemene Inlichtingen- en Veiligheidsdienst* or AIVD) and the Military Intelligence and Security Service (*Militaire Inlichtingen- en Veiligheidsdienst* or MIVD). The Minister of the Interior and Kingdom Relations is responsible for the AIVD; the Defence Minister oversees the MIVD.

The central purposes of the AIVD and MIVD are 'to collect and process data in order to perform risk and threat assessments, to collect (foreign) intelligence, investigate individuals or organizations, protect vital sectors and conduct security screenings'.[25] The aim of the ISS Act 2017 was to make the legal instruments for the AIVD and MIVD to accomplish their tasks up to date and make the legal framework 'ECHR-robust'.[26]

The second chapter of the ISS Act 2017 emphasises the division between military (MIVD) and civil (AIVD) intelligence and security activities. The latter reports to the Ministry of Defence and the former reports to the Ministry of the Interior and Kingdom Relations. The services 'conduct their work independently of law enforcement services'. The ISS Act 2017 highlights the distinction between regular powers

---

[24] C.W. Hijzen and Peter Koop, Blogpost on Intelnews.org, 'Report from Holland: cable-bound interceptions and dragnets', 24 March 2018. Internet: https://intelnews.org/2018/03/24/01-2294/.

[25] Cf. Q. Eijkman, N. van Eijk, and R. van Schaik, 'Dutch national security reform under review: sufficient checks and balances in the Intelligence and Security Services Act 2017?' (Amsterdam University 2018), 15.

[26] Dielemans, 'De Wiv 2002 en Wiv 2017', passim.

and special powers. By labelling certain powers as 'special', the act intends to 'limit the use of certain powers to highly prioritised tasks, while regulating such powers more carefully because of their raised impact on human rights'. Special powers can only be used for a more narrow set of tasks, such as 'defending a continuing democratic legal order, protecting national security, investigating other countries and their militaries, maintaining international legal order, or specific military activities'.[27]

Every four years, the Prime Minister, the Minister of Defence and the Minister of the Interior and Kingdom Relations produce a policy document that assesses the intelligence requirements of the ministries and document the priorities that exist 'when performing the tasks for which the use of special powers is permitted'. This is a legally binding document, and it includes the 'investigatory assignments that the services must perform during the four-year period'.[28]

Regular powers include: collecting information available through OSINT and social media; collecting intelligence via informants; collecting intelligence from sources. Special powers include: encryption, decryption and back doors; DNA analysis; intercepting communications; conducting surveillance; searching enclosed spaces or closed objects; investigating objects to establish a person's identity; hacking.

The third chapter of the Act deals with the processing of data. All services must adhere to certain rules. These include that all gathered data must serve a certain purpose, must be collected in a careful manner in accordance with the law, and the reliability of the source must be indicated. Data on persons may only be processed if there is a strong suspicion that the person represents a danger to the democratic rule of law (*rechtsorde*) or state security. However, the Dutch Data Protection Act (DPA) 'does not apply to the Dutch security and intelligence services' as these services are excluded from its scope. So it is unclear 'which data subjects may be affected by the ISS Act 2017' (Eijkman et al. 18). Also new is the 'provision allowing interference via a device of a third technically related party, who is not a target' (Eijkman et al. 24). Along the same lines, 'Providers of communication services' must assist intelligence and security services.

An important difference between the 2002 and 2017 Acts is that in the 2002 Act, 'untargeted bulk interception of communications was only permitted for non-cable-bound communications', and 'interception of cable-bound communications' was prohibited.[29] (Eijkman et al. 20). The 2017 Act avoids technological distinctions, and 'bulk cable-bound interception is now permitted under various safeguards'. Heads of the services must ensure the quality of data processing, including models and algorithms used. So overall, in the ISS Act 2017, there is now a legal basis for the

---

[27] Eijkman, Van Eijk, and Van Schaik, 'Dutch national security reform', 16.

[28] Ibidem, 22.

[29] Ibidem, 20.

interception of both cable-bound and non-cable-bound communications if it is directed at 'specific persons, organizations, numbers (such as a telephone number) or other technical characteristics involved' (Eijkman et al. 21). Safeguards have mostly remained the same, such as prior authorisation (Minister) and 'assessment of the use of the powers by the Assessment Committee on the Use of Powers', an ex ante oversight committee.

This introduction of bulk communications interception for 'investigation related purposes' was the most controversial aspect of the ISS Act 2017. No special authorisation is needed for automated analysis of big data, unless it is targeting one person. No action against a person may be taken solely based on automated analysis. There is also a set of powers that covers the transfer of data. Data can only be transferred internally if the transfer is necessary for certain tasks. External data transfers must be recorded, and there is a more detailed framework in place for that. There is a new provision regarding automated data analysis which is now codified on a legal basis.

Chapter six of the ISS Act 2017 deals with the cooperation between services and with other institutions. The Act also regulates cooperation with national and international authorities in more detail. The AIVD and MIVD are allowed to cooperate and share data as required. Overall, whether the Dutch services can cooperate with foreign services has not changed much; cooperation depends on whether the foreign service is in a democratic country, the level of respect for human rights, and the level of data protection. There are, however, stronger safeguards for the provision of unevaluated data, e.g. raw data in bulk. There needs to be ministerial consent for cooperation.

Chapter seven of the ISS Act 2017 deals with oversight, complaints and whistleblowing. The CTIVD, an independent body responsible for monitoring the lawful implementation of the ISS Act 2002, remains and it now monitors the implementation of the ISS Act 2017. It is composed of two separate departments, one for oversight and one for complaints and whistleblowing. The National Ombudsman lost its authority under the ISS Act 2017. The legal framework places emphasis on the requirements of constitutional and human rights law regarding rights that may infringe the privacy of citizens.[30]

V. The police and organised crime[31]

The police work within the framework of the Police Act 2012, the Code of Criminal Proceedings (*Wetboek van Strafvordering*) and the Code of Criminal Law

[30] Dielemans, 'De Wiv 2002 en Wiv 2017', passim.

[31] The author is grateful to Pietjan den Hollander for his input for this section.

(*Wetboek van Strafrecht*).[32] Organised crime is one of the areas the police has fought against in the last few centuries, as was illustrated in the introduction to this contribution. In recent trend reports, organised crime – ranging from drug and sex trafficking, fraud, to serious environmental crimes – was considered as a major threat to public order.[33]

In a recent publication on an international approach against organised crime in Europe, a Joint Investigation Team (JIT), supported by Eurojust and Europol, is considered as a recent innovation in the fight against organised crime.[34] The report shows that European cooperation is key to tackling this issue, as the division of activities across nations makes it difficult to identify, investigate and take down the network as a single nation. Eurojust provided funding and facilitated the JIT, while Europol helped in analysis.

In terms of criminal punishment, the Ministry of Justice finds that in three-quarters of the cases of organised crime a lighter sentence was given than the Public Prosecutor pled for. On average this difference is fifteen months initially and seventeen-and-a-half months on appeal. The difference between the first sentence and the one on appeal averages nine months, in favour of the defendant. In the lower court the demanded sentence averages 66 months, while the sentence averages 49 months. In the end, sentences after appeal are generally two years shorter than the demand in the first court. This difference occurs due to partial acquittal and the longer duration of the process in appeals.[35] With regard to the impact, Dutch authorities conclude that in general they do not have the manpower and means to investigate leads extensively, and that local authorities have a lack of awareness.[36]

VI. National security

The AIVD is obliged – in the name of national security – 'to do research in relation to organisations and persons that, through the goals they pursue or through their activities, give rise to the suspicion that they form a threat to the survival of the

---

[32] Internet: https://wetten.overheid.nl/BWBR0031788/2013-05-01; https://wetten.overheid.nl/BWBR0001903/2013-04-01/#BoekTweede_TiteldeelI_AfdelingEerste_Artikel141; https://wetten.overheid.nl/BWBR0001854/2013-04-01/#BoekEerste_TiteldeelIIA_AfdelingEerste_Artikel36e.

[33] Internet: https://www.politie.nl/binaries/content/assets/politie/algemeen/nationaal-dreigingsbeeld-2017/nationaal-dreigingsbeeld-2017.pdf.

[34] Internet: https://www.om.nl/vaste-onderdelen/zoeken/@104625/gecoordineerd/.

[35] Internet: https://www.politieenwetenschap.nl/publicatie/politiewetenschap/2017/geiste-en-opgelegde-straffen-bij-de-strafrechtelijke-afhandeling-298/ .

[36] Internet: https://www.politieenwetenschap.nl/publicatie/politiekunde/2018/ondermijning-door-criminele-weldoeners-309/.

democratic order or the security or other important interests of the state'.[37] Their military counterpart the MIVD focuses on the potential and armed forces of other countries in order to safeguard the deployment of Dutch troops. All their other activities are also bound to 'national security'.[38]

This idea of 'national security' is central to the division of work between the police and Justice Department on the one hand, and the intelligence community on the other. What it exactly means, however, is unclear: a thorough conceptualisation of national security is lacking. The National Coordinator for Counterterrorism and Security (NCTV) argues that national security is at stake if 'one or more vital interests of the Dutch state and/or society is threatened to such an extent that (potential) social disruption will follow' – these vital interests being territorial integrity, economic/ecological/physical security, and social and political stability.[39]

The AIVD describes it as a 'difficult concept', lacking universal meaning, but comprising 'all the values, rules, and laws we deem important in our country'; according to its annual reports, phenomena such as terrorism, the proliferation of nuclear weapons, and espionage against the Dutch state can put national security at risk. It comprises the entire Kingdom of the Netherlands; 'local and regional topics, such as local antidemocratic parties, can affect [national security] when they encapsulate the national level'.[40]

What national security is, seems to be defined by the phenomena that can threaten it, and although organised crime – as explained above – was considered as such in the past, it is not anymore. Despite the vagueness surrounding the concept (when is a 'vital interest' such as physical security actually threatened? What 'values' are deemed important by 'us', who is 'us' exactly? Etc. etc.), national security is considered as the domain of the intelligence and security services, whereas the police and the Justice Department keep themselves busy fighting 'ordinary' criminal and security matters.

The orientation of the intelligence and security services is ante-factum. This means that the AIVD and MIVD are supposed to act before a tangible threat to national security occurs. They have to collect specific information at a very early stage and the law allows them to act much earlier than the judiciary authorities would be able

---

[37] Article 8 of the Act for the Intelligence and Security Services 2017, Internet: https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/publicaties/2018/01/31/tekst-wiv-2017/Tekst+Wiv+2017.pdf.

[38] Article 10 of the Act for the Intelligence and Security Services 2017, Internet: https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/publicaties/2018/01/31/tekst-wiv-2017/Tekst+Wiv+2017.pdf.

[39] Internet: https://www.ensie.nl/nationaal-coordinator-terrorismebestrijding-en-veiligheid/nationale-veiligheid and https://www.nctv.nl/organisatie/nationale_veiligheid/index.aspx.

[40] Website General Intelligence and Security Service Internet: https://www.aivd.nl/onderwerpen/het-werk-van-de-aivd/vraag-en-antwoord/wat-is-nationale-veiligheid.

to. The purpose of intelligence gathering is to neutralise a threat, not to investigate and prosecute. Criminal investigation and prosecution, on the other hand, are post-factum oriented. Their main task is to investigate crimes that have been committed and bring suspects to court. In practice, however, both the criminal investigation and prosecution authorities and the intelligence community might be interested in the same people and organisations – for, again, different reasons.

Overall, however, these different values make for markedly different regimes. Whereas the intelligence and security services can be allowed to use a special power, such as a hack, based on the suspicion that this will provide them with information that would help them prevent a violation of national security (e.g. a possible terrorist plot), the police will need to submit more concrete and tangible evidence before they are allowed to do so. This is legitimated by a 'small, chance – high impact' argument: even though the chances of terrorist attacks, military invasions, and other violations of 'vital interests' are statistically low, the impact of their occurrence is considered so high, and their consequences so considerable, that the state is permitted to use such infringing powers if they help in protecting national security.[41] Infringing on citizens' privacy through tapping their telephone communications or running an agent in their proximity is considered as proportionate.

This is also considered justified because the use of these special powers in the name of national security only serves to collect specific information that helps the state protect national security. Their use is therefore *without legal consequences for the individual*. In the domain of criminal investigation and prosecution these same instruments can be used, but they serve a different purpose: they are employed to find legal evidence as a basis for prosecution.

VII. Counterterrorism

The separation of spheres between both worlds still exists today, even though different phenomena brought the police, the Justice Department, and the intelligence community closer together in recent times. Since the attacks of 9/11, both the intelligence and security services and the police are very active in the field of counterterrorism and there are several indications that the separation of spheres is breaking down, at least in this specific domain.

To begin with, the phenomenon of terrorism itself is to some extent inherently criminal. Sometimes criminal networks seem to be connected to terrorist activities, for example when criminal activities are used to finance terrorism or when (petty)

---

[41] G. de Valk, *Dutch intelligence. Towards a qualitative framework for analysis: with case studies on the Shipping Research Bureau and the National Security Service (BVD)* (Groningen 2005) 69.

criminals become terrorists. As a result, intelligence services are also active in discovering the clandestine criminal activities of terrorists or extremists. This can also be the case in the field of arms, drugs or human trafficking. It is undisputed that the Dutch intelligence and security services are able to play a role in this field by means of intelligence gathering and providing analyses.

As a result, the exchange of information between the police and Justice Department on the one hand, and the intelligence community on the other, has been improved in recent years. If the AIVD, for example, comes across information that in their eyes should be reviewed by the Public Prosecution Office, as a by-product of an intelligence operation – or in order to disrupt a terrorist plot, for example – it can forward this information by sending an official message (*Ambtsbericht*). If the Public Prosecutor then wants to use this information to prosecute someone, he must then start a (new) criminal investigation and collect evidence in the course of this investigation. As a result of the ever-increasing terrorist threat some legal adjustments have been made in the last fifteen years, but only in this specific domain. Under certain circumstances intelligence about terrorist activities can be admitted as evidence in a criminal trial and intelligence officers can be summoned as protected witnesses in court. In 2004, the Court of The Hague ruled that information 'can be the start of applying initial investigation powers such as the arrest of suspects and the searching of houses, if that information results in a reasonable suspicion'.[42] In practice, this means that the Dutch intelligence community, particularly the AIVD, sends out *ambtsberichten* to the Public Prosecutor.

Both the intelligence community and the police are strongly focused on the 'subject of interest' (SOI) and their approach is network-oriented. Which individuals and which networks are prone to and capable of staging terrorist attacks? They therefore also both run agents and informants, which might result in them being interested in the same person or network. This is why both parties regularly meet and discuss their activities, in order to prevent, for example, the same informants and agents being approached or phones being tapped at the same time. To this end, intensive consultation takes place in the so-called Counterterrorism Coordination Meeting (*Algemeen Overleg Terrorismebestrijding* or AOT) between the Public Prosecutor and the AIVD, under the direction of a National Anti-Terrorism Public Prosecutor.

In addition, the so-called Counter Terrorist Infobox (CT Infobox) was created, a 'black box' in which all available information about certain high-risk terrorists is brought together in order to formulate in a closed setting advice on how the risk of a certain person could best be mitigated. Working from the building of the General Intelligence and Security Service, ten partners in the counterterrorism domain, besides the civil intelligence and security service, for example the Public Prosecution Office, the police, tax authorities, and the National Coordinator for Counterterrorism

---

[42] Hof's-Gravenhage, 21 June 2004, LJN, AP2058.

and Security, discuss individual cases in the counterterrorism domain. They combine their information position, intelligence and expertise on networks and individuals on their respective radars, in order to discuss whether and, if so, how the government should act against specific individuals who might pose a threat in terms of terrorism.

The specific information and intelligence are not shared with anyone outside the CT Infobox, not even the 'home organisations', nor is a 'master file' on specific targets created. 'What's in the box, stays in the box', the adage goes. The only thing that comes out of the CT Infobox is specific advice to a specific government body or organisation, be they a CT Infobox partner or for example a municipality. First, the CT Infobox can recommend to provide information to one or more partners (*verstrekkingsadvies*). Second, it can 'alert' an organisation about an individual in order to act, e.g. to start an investigation (*attenderingsadvies*). And third, the CT Infobox can recommend an 'individual centred approach' (*persoonsgerichte aanpak*).[43]

These are all legal and organisational adjustments that relate to terrorism. Countering terrorism is an undisputed task, both for the intelligence world and the field of police and prosecution. In recent times, organised crime has not been considered as a threat to national security – it is therefore not considered an issue for the intelligence community in itself.

In recent years, however, the discussion about organised crime and the integrity of government has resurfaced. This time 'undermining' is the buzz word and the topic of interest is Brabant, a province in the south of the Netherlands, where major drug networks are active. Threatening mayors and other administrators – in some cases even committing arson attacks on town halls and other public facilities – they echoed the discussions of the 1990s. So far, however, it is only a discussion. In recent debates about the new Act for the Intelligence and Security Services a greater involvement of the intelligence and security services in combating organised crime, no such arguments were put forward.

VIII. Conclusion

In conclusion, despite the recent political debate about the involvement of intelligence collection methods abroad in countering organised crime, the Dutch intelligence and security services are not engaged in fighting organised crime. This has been traditionally considered as the prerogative of the police and the Justice Department, who in the name of protecting the rule of law developed laws, institutions, instruments and practices to investigate and prosecute criminal acts. Although the problem of organised crime has been around for centuries, as it has been in other

---

[43] C. de Poot and S. Flight, *Ruimte om te delen: de CT Infobox tien jaar in werking* (WODC-rapport) (Den Haag 2015) 8–11, passim.

states, it was not until the late 1980s that the police started to intensify their operations against organised crime. The main goal was to improve their understanding of the way criminal networks were run and how they operated. Because the police also used 'intelligence techniques' such as agent handling and running informants, this brought the police de facto closer to the world of intelligence.

This did not imply that the intelligence and security services – the national security establishment – saw organised crime as a phenomenon that fell within their responsibility. Historically, there runs a deep divide between both worlds. Because organised crime was considered as exactly that – a crime, and therefore the business of the police and the Justice Department, the intelligence community did not bother, the notable exception being the decade between 1990 and 2000, when the security service was to some extent looking for new fields of study and legitimate reasons for a continued existence in the post-Cold War world.

This separation of spheres stems from the Second World War and led to the existence of two very different regimes in terms of institutions, organisations, concepts, and practices. The work of the police and the Justice Department is connected to fighting (organised) crime, whilst the intelligence and security services investigate in order to protect national security. The police are interested in evidence of crime, and focuses on criminal or other individual motivations; the intelligence community seeks to avert catastrophic events that might harm national security and focuses on the ideological or political-religious motivations, intentions, and actions of groups, individuals and states in relation to national security. They can use the same means, but under different circumstances.

'National security' is the key concept here. The intelligence community can perceive organised crime as a threat to national security, as it had done in the 1990s, but since 2000 it has not done so. Only in the domain of counterterrorism, where the strict divide seems to become increasingly (semi) permeable, we see an interest of the intelligence community in organised crime. But in itself, organised crime is considered as a phenomenon that is 'merely' criminal – vital interests, the democratic order, or state security are not considered as being at stake.

Architecture and role of intelligence services in Romania

Johanna Rinceanu

A. Introduction

Intelligence is not an innovative response to terrorist attacks. Intelligence services already existed before 9/11: They existed in dictatorships, oligarchs, monarchies and democracies alike.[1] Terrorist attacks and in particular 9/11, however, changed the landscape of the intelligence community: Romania adopted – like many other countries worldwide – new legislation on preventing and combating terrorism, terrorist financing, organized crime, and human trafficking.[2]

---

[1] *Beer*, Die Nachrichtendienste in der Habsburger Monarchie. In: Zeitschrift für Polizeiwissenschaft und polizeiliche Praxis (SIAK-Journal), 2007, (3), S. 53 (53–63).

[2] *Matei*, Romania's Intelligence Community: From an Instrument of Dictatorship to Serving Democracy. In: International Journal of Intelligence and CounterIntelligence 20, no. 4 (2007), p. 648.

Romania's fight against international terrorism, on the one hand,[3] and the aspiration to be part of NATO[4] and the EU,[5] on the other hand, led to a change in the way its intelligence services work. There has been an increase in cooperation between the Romanian intelligence services and the Romanian law enforcement agencies, between Romanian intelligence services and foreign intelligence services, as well as between the Romanian intelligence services and foreign law enforcement agencies. The greatest challenge in such forms of wide-ranging cooperation is keeping the balance between effective intelligence in the service of national security and the right to a fair trial and respect for the human rights of the accused. Independent oversight bodies have to monitor this balance and provide for legal safeguards to ensure the right of the accused person to a fair trial according to international human rights law. Such independent oversight bodies could be the parliament, inspectors-general, or courts. The different national oversight bodies need to cooperate internationally in the same wide-ranging way as intelligence services do in order to ensure accountability and to guarantee the constitutional principle of the rule of law.[6]

This article provides an overview of the architecture and role of intelligence services in Romania. First, the main features of the national security are presented (B.). In the following section, the current structure of the intelligence services is illustrated without losing sight of the historical background (C.). Subsequently, the concrete interaction between intelligence services and law enforcement is examined (D.). The primary focus here is on the question to what extent intelligence services perform *de facto* or *de jure* law enforcement tasks and whether evidence collected by intelligence services can be admitted to criminal proceedings. This article concludes with a few thoughts about the professionalism and effectiveness of the Romanian intelligence community and its transparency and compliance with human rights (E.).

---

[3] Romania has acceded to numerous international counter-terrorism conventions and multilateral anti-terrorism conventions. For details see *Rinceanu*, National characteristics, fundamental principles, and history of criminal law in Romania. In: Ulrich Sieber/Konstanze Jarvers/Emily Silverman (eds.), National Criminal Law in a Comparative Legal Context, vol. 1.5., Introduction to National Systems, pp. 218–219.

[4] Since 2004, Romania has been a member of the political and military alliance NATO.

[5] Since 2007, Romania has been a member of the EU.

[6] The rule of law is enshrined in Art. 1(3) of the Constitution. Accordingly: "Romania is a democratic and social state, governed by the rule of law, in which human dignity, the citizen's rights and freedoms, the free development of human personality, justice and political pluralism represent supreme values, in the spirit of the democratic traditions of the Romanian people and the ideals of the Revolution of December 1989, and shall be guaranteed." The translation of the Romanian Constitution into English – as cited in this paper – has been generated from excerpts of texts from the repository of the Comparative Constitutions Project, and distributed on *constituteproject.org* available at https://www.constituteproject.org/search?lang=en&q=Romania&status=in_force&status=is_draft (last visited July 2020).

B. Main features of the national security architecture

There is a functional division in terms of separation of powers and tasks between the police, criminal investigation authorities and intelligence services. They build together the national security architecture but are, however, functionally strictly separate authorities.

The Romanian Police is part of the Ministry of the Interior (*Ministerul Afacerilor Interne*). It consists mainly of a General Inspectorate (*Inspectoratul General*), associated territorial units (*unităţi teritoriale*), a General Directorate Bucharest (*Direcţia generală de poliţie a municipiului Bucureşti*) and so-called Inspectorate Districts (*inspectoratele judeţene*).[7] The general legal framework regulating the activity of the Police is Law no. 218/2002 on the Organization and Functioning of the Romanian Police[8] and Law no. 360/2002 on the status of the police officer.[9] The task of the police is, hence, generally speaking, to protect human rights and fundamental freedoms, to protect private and public property, to prevent and detect criminal offenses as well as to maintain public safety and legal order according to the law.[10]

In order to achieve these goals, the General Inspectorate coordinates and guides the application of measures on public peace and order, is responsible for the safety of the citizen, crime prevention and combating, identification and counteracting of the criminals' actions threatening the life, freedom, health and bodily integrity of persons, private and public property, as well as other legitimate interests of the community. It collaborates with specialized institutions and authorities of the public central administration from the System for Defense, Public Order and National Security as well as with specialized structures from other states and from international organizations on preventing and combating trans-national crime. The General Inspectorate supports furthermore the establishment of an international police, runs activities of human resources management, according to the law, and coordinates the activities of international police cooperation. It ensures the representation, at the institutional level, in relationships with public institutions and authorities, collaborates with the chiefs of all the other structures of the Ministry of the Interior for the accomplishment of the tasks and measures mandated by the management of the Ministry of the Interior.[11]

The Public Ministry (*Ministerul Public*) – as part of the Ministry of Justice (*Ministerul Justiţiei*) – together with the criminal investigation organs (*organe de cercetare penală*), is the criminal investigation authority in Romania.

---

[7] Art. 5 of Law no. 218/2002.

[8] Legea Nr. 218 din 23 aprilie 2002 privind organizarea şi funcţionarea Poliţiei Române.

[9] Legea Nr. 360 din 6 iunie 2002 privind Statutul poliţistului.

[10] Art. 1 of Law no. 218/2002.

[11] See Art. 26 of Law no. 218/2002.

The legal framework for the organization of the Public Ministry is regulated by Law no. 304/2004 on the Judicial Organization.[12] The role of the Public Ministry is to represent the general interests of society and to defend the legal order and the rights and freedoms of citizens.[13] The tasks of the Public Ministry are carried out by (public) prosecutors (*procurorii*), organized in numerous offices of the prosecutor located around the country on the basis of a strict hierarchy:[14] On the top of the hierarchy is the office of the prosecutor affiliated with the High Court of Cassation and Justice; it is represented by the public prosecutor general. Immediately thereunder are offices of the prosecutor attached to the courts of appeal, followed by offices attached to the tribunals, and, finally, offices attached to the district courts. Prosecutors are responsible for coordinating and supervising criminal investigations carried out by the police. In cases involving certain serious offenses, however, such as murder (*omorul*), homicide on request (*uciderea la cererea victimei*), and torture (*tortura*), the investigation must be carried out by a prosecutor.[15] Prosecutors must carry out their activities in accordance with the principle of legality (*principiul legalităţii*), impartiality (*principiul imparţialităţii*), and hierarchical control (*principiul controlului ierarhic*), under the authority of the minister of justice.[16]

The Public Ministry is responsible, through the above-mentioned offices of the prosecutor, for criminal investigation in cases and under conditions provided by law and it participates in conflict resolution by alternative means.[17] Furthermore, it leads and coordinates investigative activities carried out by the judicial police and leads and controls the activities of other investigative bodies. The Public Ministry, in addition to being a prosecuting authority, undertakes civil action in cases provided by law, participates in court trials, appeals court decisions, protects the rights and legitimate interests of minors, disappeared persons, and other persons, contributes to preventing and fighting crime under the direction of the Ministry of Justice, analyzes factors that generate or favor criminality, elaborates and presents drafts to the Ministry of Justice regarding decriminalization, verifies the observance of the law in pretrial detention, and performs other duties provided by law.[18]

---

[12] Legea no. 304 din din 28 iunie 2004 privind organizarea judiciară.

[13] Art. 131 Romanian Constitution.

[14] Art. 131(2) Romanian Constitution.

[15] Art. 56 Romanian Code of Criminal Procedure. See *Rinceanu*, National characteristics, fundamental principles, and history of criminal law in Romania. In: Ulrich Sieber/Konstanze Jarvers/Emily Silverman (eds.), National Criminal Law in a Comparative Legal Context, vol. 1.5., Introduction to National Systems, pp. 199–200.

[16] Art. 132(1) Romanian Constitution. See also Art. 62(2) Law no. 304/2004.

[17] Art. 63 Law no. 304/2004.

[18] *Otavă*, in: Yordanova/Markov (eds.), Judicial Reform, pp. 130–132. See *Rinceanu*, National characteristics, fundamental principles, and history of criminal law in Romania. In: Ulrich Sieber/Konstanze Jarvers/Emily Silverman (eds.), National Criminal Law in a Comparative Legal Context, vol. 1.5., Introduction to National Systems, p. 200.

The Romanian intelligence community is entrusted with the covert collection of information relevant to national security. It does not provide evidence or proof. The basic task of the intelligence community is to protect Romania against terrorism, treason, assassination attempts, armed uprisings, attempts to change the border, or antisemitic or racist acts.

C. Intelligence services

1. Historical background

The first Romanian intelligence service can be traced back to the 19th century and the unification process of Wallachia and Moldova that resulted in the proclamation of the new State of Romania by *Alexandru Ioan Cuza* in 1862. From the very outset, two branches developed simultaneously within the intelligence service: One branch dealt with the collection of information within the Romanian territory, whereas the other branch dealt with the collection of information abroad.[19] The intelligence service played an important role in the stabilization of the newly formed State as well as in the implementation of the political objectives of *Cuza*. In 1865, the general staff of the armed forces (*Marele Stat Major*) developed a special (second) department responsible for collecting, analyzing and summarizing information with military content. Within the Ministry of the Interior, a General Security Office was established in 1892, which was converted into a Police and General Security Directorate (*Direcţia Poliţiei şi Siguranţei Generale*) in 1908 with the aim of identifying threats against the state.

During the First World War (1914–1918), a system of espionage and counter-espionage emerged. Due to social and political changes after the First World War, on the one hand, and territorial enlargement, on the other hand, the need arose to restructure the Romanian intelligence service. In 1917, the Safety Bureau of the Danube Delta was set up.[20] Shortly after the end of the First World War, the Secret Service of the Romanian Army (*Serviciul Secret al Armatei Române, SSIAR*) was established initially under the general staff of the armed forces and was later directed by the latter in cooperation with the National Department of Defense (*Ministerul Apărării Naţionale*).[21] The SSIAR wanted to merge the activities of

---

[19] *Manda*, Evoluţia sistemului de Securitate în România. In: Revista de Investigare a Criminalităţii 1/2016, p. 597.

[20] The Safety Bureau of the Danube Delta was disbanded already in 1920.

[21] *Manda*, Evoluţia sistemului de Securitate în România. In: Revista de Investigare a Criminalităţii 1/2016, p. 598.

the Romanian intelligence service and the external information service into one authority.[22]

Since the beginning of the Second World War and until the establishment of communism in the mid-forties, the structure of the Romanian secret service changed several times. At times the secret service was subordinated to the Ministry of the Interior, at other times to the Ministry of Defense, changing continuously denomination.[23] The first half of the communist era, i.e. from 1945 to 1964, under *Gheorghe Gheorghiu Dej* and later under *Petru Groza*, was marked by terror to remove political dissenters who were considered obstacles to the regime, whereas the second half of the communist era, i.e. from 1965 to 1989, under *Nicolae Ceauşescu*, was marked by fear of the *Securitate* rather than terror.[24] A change in the degree of repression occurred.[25]

2. The *Securitate* and its legacy

During the second half of the communist era the intelligence services were changed both in structure and character. The priority for national security became the backing of the communist regime and the industrial development of the country in the spirit of the communist ideology.[26] In this way, the *Securitate* grew into an instrument of public surveillance. A large part of the population had been intercepted. Dissidents and opponents of the regime were persecuted, tortured and eliminated. By the end of 1989, the *Securitate* employed over 15,300 officers,[27] over 23,300 officers of the security troops command (*Comandamentul Trupelor de Securitate*)[28] and had around 400,000 active informal collaborators or so-called

---

[22] *Manda*, Evoluţia sistemului de Securitate în România. In: Revista de Investigare a Criminalităţii 1/2016, p. 599.

[23] See *Manda*, Evoluţia sistemului de Securitate în România. In: Revista de Investigare a Criminalităţii 1/2016, p. 599.

[24] *Matei*, Romania's Transition. In: Thomas C. Bruneau/Stefan C. Boraz (eds.), Reforming Intelligence: Obstacles to Democratic Control and Effectiveness, 2007, p. 221 reports that the "Securitate succeeded in instilling in the population a 'fear of their own shadow' and the belief that the visible presence of officers was only an infinitesimal element of an omnipresent network of officers, agents, informers, and collaborators who were watching them. It was indeed a state of mind as much as the instrument of state oppression."

[25] *Deletant*, Ceauşescu and the Securitate, Coercion and Dissent in Romania, 1965–1989, p. 1.

[26] *Manda*, Evoluţia sistemului de Securitate în România. In: Revista de Investigare a Criminalităţii 1/2016, p. 602.

[27] *Söller*, Im Spannungsfeld von "nationalen" und "europäischen" Ansprüchen? Eine Betrachtung des Nationalen Rates für das Studium der Securitate-Archive In Rumänien. In: JHK (2014), p. 109.

[28] *Deletant*, Ceauşescu and the Securitate, Coercion and Dissent in Romania, 1965–1989, Preface, p. xiii.

informants.[29] The *Securitate* became omnipresent. Under *Nicolae Ceauşescu*, the *Securitate* became the largest secret service in Eastern Europe compared to population size.[30]

After the fall of Communism in December 1989, the *Securitate* was entirely disbanded. Wiretapping and recording centers were closed overnight. The interception of private communications was banned by law – a ban that lasted until 1991.[31] In the aftermath, the intelligence services in Romania experienced a stony path of transition: From a ubiquitous Communist *Securitate* to a democratic intelligence community.[32]

As in many former non-democratic countries, Romania's new designed intelligence community carried the "stigma" of its past as it was built on the ruins of the *Securitate*.[33] The fact that a certain number of former *Securitate* personnel held a position in the new intelligence community contributed strongly to this stigmatization. It would have been, however, remote and hence impossible to hire only new personnel, considering the lack of adequate staff education. Romania, as a developing democracy after the fall of Communism, required a new generation of intelligence personnel.

3. New architecture

In 1991, Law No. 51/1991 on the National Security of Romania created a new legal framework for a new intelligence architecture.[34] Accordingly, the Romanian intelligence community consists to date of six services and ministerial substructures charged with intelligence collection: The Romanian Intelligence Service (SRI) – as the essential intelligence service responsible for internal security, the Foreign Intelligence Service (SIE), the Guard and Protection Service (SPP), the Special

---

[29] *Deletant* reports about an excess of 400,000 informants citing Virgil Măgureanu, the former Director of the SRI. In: Ceauşescu and the Securitate, Coercion and Dissent in Romania, 1965–1989, Preface, p. xiv.

[30] *Matei*, Romania's Intelligence Community: From an Instrument of Dictatorship to Serving Democracy. In: International Journal of Intelligence and CounterIntelligence 20, no. 4 (2007), p. 631.

[31] See *Watts*, Control and Oversight of Security Intelligence in Romania. In: Born, Hans/Caparini Marina (eds.), Democratic Control of Intelligence Services – Containing Rogue Elephants, pp. 48–49.

[32] For more details see *Matei*, Romania's Intelligence Community: From an Instrument of Dictatorship to Serving Democracy. In: International Journal of Intelligence and CounterIntelligence 20, no. 4 (2007), pp. 629–660.

[33] *Bruneau/Matei*, Intelligence in the developing democracies: the quest for transparency and effectiveness. In: Loch K. Johnson (ed.), The Oxford Handbook of National Security Intelligence, p. 760.

[34] Legea nr. 51 din 29 iulie 1991 privind securitatea naţională a României, republished in M.Of. no. 190 of 18 March 2014.

Telecommunication Service (STS), the ministerial General Directorate for Internal Security (DGPI), and the Directorate for General Information of the Army (DGIA).

The Supreme Council of National Defense (*Consiliul Suprem de Apărare a Ţării, CSAT*) is the autonomous administrative authority in Romania with the task of analyzing and assessing the national security status and – as a further step – organizing and coordinating the activities related to the country's defense and national security. The President of Romania chairs the Supreme Council of National Defense.[35] The activity of the Council is examined by Parliament as oversight body.

a) Romanian Intelligence Service (SRI)

The Romanian Intelligence Service (*Serviciul Român de Informaţii, SRI*) is the direct successor of the *Securitate*.

The task of the SRI is to protect democratic values and promote the national interest of Romania and of its allies in order to ensure national security, the observance of civil rights and freedoms and the defense of the rule of law. To achieve this task, the SRI collects data and analyzes all national security risks, challenges and threats, including the threat of terrorism. Its specific data collection activity is frequently in the fields of economic security, protection of public order and constitutional values, counterespionage, cross border threats – such as activities of organized crime networks, smuggling, illegal migration, drug trafficking, cybercrime, proliferation of CBRN weapons, clandestine programs for the provision of conventional or weapons of mass destruction and carrier vectors – cyber intelligence, prevention and countering of terrorism.[36] While the SRI can support the criminal investigation and prosecution bodies by providing information regarding *inter alia* the above-mentioned fields of crime, the SRI is not allowed to carry out acts of criminal investigation by itself, nor detain or take someone into preventive custody.[37]

In fulfilling its tasks, the SRI cooperates with the SIE, the SPP, the Defense Ministry's Directorate of Defense Intelligence, the General Directorate of Intelligence and Internal Protection of the Interior Ministry, the Ministry of Justice, the Public Ministry, the Ministry of Foreign Affairs, the Ministry of Economy and Finance, the General Directorate of Customs as well as other bodies of public administration. These institutions are obliged to provide each other with the support necessary for the execution of the duties required by law.[38] Apart from that, with the approval of

---

[35] See Art. 92(1) of the Constitution.

[36] See the Report on the Activity of the Romanian Intelligence Service in 2012. Available at https://www.sri.ro/assets/files/reports/2012/REPORT_on_the_Activity_of_the_Romanian_Intelligence_Service_in_2012.pdf (last visited January 2020).

[37] See Art. 13 Law no. 14/1992.

[38] See Art. 14 Law no. 14/1992.

the Supreme Council of National Defense, the SRI can establish ties with similar institutions from abroad.[39]

The staff of the SRI consists of permanent military personnel and civilian staff performing operational and administrative tasks.[40]

The legal framework for the activity of the SRI is provided by the Constitution and a plethora of other laws.[41]

b) Foreign Intelligence Service (SIE)

The Foreign Intelligence Service (*Serviciul de Informații Externe, SIE*) is specialized in gathering information from *abroad*. It is responsible for national security, the defense of Romania and its interests.

SIE's mission is to collect relevant information for the national security of Romania, information which constitutes the basis for decisions by the state authorities, early warning of risks and threats and strategic assessments of the international security environment and conducting operations to defend and promote Romania's interests. The activity of the SIE is as a state secret highly confidential, and the information sources, methods and means of work may not be disclosed to anyone or in any circumstance.[42] The SIE is authorized to use covert legal entities (*persoane juridice sub acoperire*) established under conditions of law, to use specific methods, to create and have adequate means to obtain, verify, protect, evaluate, use and store data and information concerning national security.[43] Under certain conditions, the SIE conducts field interventions abroad.[44]

In order to fulfill its tasks and to ensure a unified and coherent policy of the intelligence community at the external level, the SIE cooperates with ministries, public bodies and other legal entities established by the Supreme Council of National

---

[39] See Art. 15 Law no. 14/1992.

[40] See Art. 27 Law no. 14/1992.

[41] See Law no. 51/1991 on the National Security, Law no. 14/1992 on the Organization and Functioning of the SRI, Law no. 535/2004 on Prevention and Countering Terrorism, Law no. 544/2001 on Free Access to Public Information, Law no. 182/2002 on the Protection of Classified Information and the Convention for the Protection of Human Rights and Fundamental Freedoms as well as the Additional Protocols to the Convention.

[42] Art. 10(2) Law no. 1/1998.

[43] Art. 10(1) Law no. 1/1998.

[44] *Matei*, Romania's Anti-Terrorism capabilities: Transformation, Cooperation, Effectiveness. In: Journal of Defense Resources Management, Vol. 3, Issue 1 (4)/2012, p. 41, exemplifies: "The SIE created a special intervention unit for operations abroad in order to free hostages and to ensure the guard and protection of embassies outside of Romania."

Defense.[45] With the approval of the Supreme Council of National Defense, the SIE can establish ties with similar institutions from abroad.[46]

The SIE's activity is organized and coordinated by the Supreme Council of National Defense. The control over the activity of the SIE is exercised by Parliament as oversight body while maintaining the secrecy of the means and sources of information.[47] Parliamentary control aims to verify the conformity of the activities of the SIE with the Constitution and Romanian state policy.

The staff of the SIE consists of military personnel, contract military personnel and civilian personnel.[48]

The legal framework for its activity is provided by the Constitution and a multitude of other laws.[49]

c) Guard and Protection Service (SPP)

The Guard and Protection Service (*Serviciul de Protecţie şi Pază, SPP*) – *nomen est omen* – is specialized in providing protection for Romanian dignitaries, foreign dignitaries during their stay in Romania, and their families, within its legal competence. It furthermore provides guard for the headquarters and residences of the above-mentioned dignitaries in accordance with the decisions of the Supreme Council of National Defense.[50] The SPP also protects Romanian dignitaries outside the national territory in cooperation with special services from the host countries[51] and has an Anti-Terrorist Intervention Section dedicated to the prevention and combating of terrorist attacks against dignitaries and buildings they are protecting.

In order to carry out its tasks, the SPP collaborates with the Ministry of National Defense, the Ministry of the Interior, the SRI, the SIE, the Special Telecommunica-

---

45 Art. 4(1) Law no. 1/1998.

46 Art. 4(2) Law no. 1/1998.

47 Art. 3(1) Law no. 1/1998.

48 Art. 13 Law no. 1/1998.

49 See Law no. 1/1998 on the Organization and Functioning of the SIE, Law no. 51/1991 on the National Security, Law no. 415/2002 on the Organization and Functioning of the CSAT, Parliamentary decision no. 44/1998 on the Establishment, Organization and Functioning of the special parliamentary commission for the control of the activity of the Foreign Intelligence Service, Law no. 80/1995 on the status of Military Personnel, Law no. 53/2003 on Labor Code, Law no. 384/2006 on the Status of Soldiers and professional Military, Law no. 544/2001 on Free Access to Public Information, Law no. 182/2002 on the Protection of Classified Information, and governmental decision no. 585/2002 on the approval of National Standards for the protection of classified information in Romania, Law no. 535/2004 on the Prevention and Combating of Terrorism and the Convention for the Protection of Human Rights and Fundamental Freedoms as well as the Additional Protocols to the Convention.

50 Art. 1 Law no. 191/1998.

51 Art. 5 Law no. 191/1998.

tions Service as well as with other specialized ministries and bodies of the central and local public administration.[52] It can establish ties with similar structures from other countries and can sign treaties at department level and technical agreements with international bodies in the field of cooperation on protection, guard and personnel training with the preliminary approval of the Supreme Council of National Defense.[53]

The activity of the SPP is organized and coordinated by the Supreme Council of National Defense and is controlled by Parliament though the Committees for Defense, Public Order and National Security. The operative activity of the SPP constitutes a state secret.[54]

The SPP has a military structure and is part of the national defense system. Its personnel consists of military personnel and civil employees. The personnel of the SPP are authorized, on a case by case basis, to carry and use firearms, weapons and other means of protection and intimidation in order to accomplish the missions assigned by the Service as well as for self-defense purposes, under the conditions stipulated by law. [55]

The legal framework for the SPP's activity is provided by the Constitution and a number of other laws.[56]

d) Special Telecommunications Service (STS)

The Special Telecommunications Service (*Serviciul de Telecomunicații Speciale, STS*) is the central specialized body that organizes, conducts, carries out, controls and coordinates the activities in the field of special telecommunications for public authorities in Romania and for other users provided by the law. The STS provides national signals intelligence.[57]

---

[52] Art. 4(1) Law no. 191/1998.

[53] Art. 6 Law no. 191/1998.

[54] Art. 31(1) Law no. 191/1998.

[55] Art. 27 Law no. 191/1998.

[56] See Law no. 191/1998 on the Organization and Functioning of the SPP, Law no. 80/1995 on the status of Military Personnel, Law no. 51/1991 on the National Security, Law no. 535/2004 on the Prevention and Combating of Terrorism, Law no. 17/1996 on the regime of Firearms and Ammunition, Law no. 295/2004 on the regime of Weapons and Ammunition, Law no. 544/2001 on the Free Access to Information of Public Interest, Law no. 333/2003 on the Protection of Objects, Assets, Values and Protection of Persons, Law no. 182/2002 on the Protection of Classified Information, Law no. 585/2002 for the approval of National Standards for the Protection of Classified Information in Romania and the Convention for the Protection of Human Rights and Fundamental Freedoms as well as the Additional Protocols to the Convention.

[57] *Matei*, Romania's Intelligence Community: From an Instrument of Dictatorship to Serving Democracy. In: International Journal of Intelligence and CounterIntelligence, 20, no. 4, 2007, p. 634.

The STS' task is to ensure communications and information technology secured services for the Romanian authorities, by developing and managing communications networks and information systems based on interoperability, standardization and security principles. Users of the special telecommunications networks are the Romanian Parliament, the Romanian Presidency, Romanian Government, institutions active in the field of defense, national security and public order, central and local public administration and/or their subordinated units that carry out activities of national public interest, legal authority (such as the Supreme Court of Justice, Public Ministry, Supreme Council of Magistracy), the Romanian Court of Accounts, the Romanian Constitutional Court and the governing structures within governmental and non-governmental organizations of national interest.[58]

In order to fulfill its tasks, the STS collaborates with institutions in the field of defense, national security and public order, with the Ministry of Communications and coordinates with the autonomous authorities, with the operators and providers of telecommunications services authorized by the Ministry of Communications, as well as with other public authorities of the state. With the approval of the Supreme Council of National Defense, the STS can establish ties with similar institutions from abroad.[59]

The activity of the STS is organized and coordinated by the Supreme Council of National Defense and controlled by Parliament.[60]

The institution has a military structure and is part of the national defense system. The staff of the STS consist of military and civilian personnel.[61]

The Special Telecommunications Service operates in accordance with the Romanian Constitution and laws of the country, the decisions of the CSAT and the government, as well as general military regulations.[62]

---

[58] See Annex no. 1 of Law no. 92/1996 on the Organization and Functioning of the Special Telecommunications Service.

[59] Art. 4 Law no. 92/1996 on the Organization and Functioning of the Special Telecommunications Service.

[60] Art. 2 and Art. 3 Law no. 92/1996.

[61] Art. 12 Law no. 92/1996.

[62] Its core legal framework consists of Law no. 92/1996 on the Organization and Functioning of the STS, Law no. 76/1993 for the ratification of the Constitution and ITU Convention, Law no. 544/2001 on free access to public information, Law no. 455/2001 on electronic signature, Law no. 182/2002 on protection of classified information, Law no. 506/2004 on personal data processing and privacy protection in the field of electronic communications, Law no. 190/2018 on measures implementing the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing the Directive 95/46/EC, and Law no. 225/2018 amending and supplementing the Government Emergency Ordinance no. 98/2010 on the Identification, Designation and Protection of Critical Infrastructure.

e) General Directorate for Internal Security (DGPI)

The General Directorate for Internal Security (*Direcţia Generală de Protecţie Internă, DGPI*) is the criminal intelligence agency of the Romanian Ministry of Internal Affairs. The DGPI collects and analyzes data on terrorist threats and organized crime.

f) General Directorate for Defense Intelligence (DGIA)

The General Directorate for Defense Intelligence (*Direcţia Generală de Informaţii a Apărării, DGIA*) was founded in 1999 and is Romania's *military* intelligence agency subordinated to the Ministry of National Defense.

The DGIA is organized into two special directorates: Directorate for Military Intelligence – foreign intelligence (*Direcţia Informaţii Militare*) and Directorate for Military Security – counter-intelligence (*Direcţia Siguranţă Militară*). The Directorate for Military Intelligence carries out activities in the field of external military information, as well as information for defense diplomacy, and ensures the provision of timely information – alerting the military and politico-military decision-making organs on the risk factors, threats and challenges to national security. The function of the Directorate for Military Security is to identify, document and counter the risks and threats to national security in the military field in order to protect the personnel, information, assets, activities and structures of the Ministry of Defense.[63]

The DGIA's general mission is to collect, process, evaluate, analyze, store and use information and data on all security risks, challenges and threats – including cyberthreats or cyberattacks – that may affect Romania's security from a national defense perspective.[64] It is responsible for ensuring the protection of security information and cryptographic activities as well as the geographical clarifications required by the military.[65] The DGIA furthermore guards and protects facilities, assets, leaders and personnel, both in Romania and abroad as well as all foreign military facilities and personnel operating on the Romanian territory.[66] The DGIA operates undercover.

The DGIA cooperates with the SRI, the SIE, the SPP as well as with the STS in areas such as classified information protection and satellite communications

---

[63] See *Savu*, Direcţia Generală de Informaţii a Apărării – Present şi Perspective. In: Infosfera, Annul I, nr. 3/2009, p. 15.

[64] *Matei*, Romania's Anti-Terrorism Capabilities: Transformation, Cooperation, Effectiveness. In: Journal of Defense Resources Management, Vol. 3, Issue 1 (4) 2012, p. 42. *Croitoru*, Rolul direcţiei generale de informaţii a apărării în sprijinul cu informaţii al categoriilor de forţe din armata României. In: Infosfera, Annul I nr. 3/2009, p. 28.

[65] *Matei*, Romania's Intelligence Community: From an Instrument of Dictatorship to Serving Democracy. In: International Journal of Intelligence and CounterIntelligence, 20, no. 4, 2007, p. 634.

[66] *Matei*, Romania`s Anti-Terrorism Capabilities: Transformation, Cooperation, Effectiveness. In: Journal of Defense Resources Management, Vol. 3, Issue 1 (4) 2012, p. 42.

monitoring.[67] It contributes to the EU strategy for the development of a common security policy, provides information support for the fight against terrorism and smuggling through the activities of the Black Sea Naval Cooperation Task Group (Blackseafor), and increases support for the fight against terrorism by strengthening cooperation with structures competent in the fight against terrorist acts and by continuing to participate with personnel and information structures in the international coalitions against terrorism.[68] In order to achieve these tasks, the DGIA contributes to different UN, NATO and EU operations.

4. Oversight and accountability

The Supreme Council of National Defense ensures the unified coordination of all activities pertaining to defense and state security, including intelligence operations. The Council coordinates and monitors activities of the SRI, SIE, and SPP and enables information and intelligence sharing among them. Oversight bodies are the Parliament and the Constitutional Court.

a) Legal oversight

The legal supervision of SRI activities is carried out through a dual mechanism: *Internal oversight* is carried out by the Legal Department of the SRI; *external oversight* is carried out by Parliament and competent judicial bodies. The SRI's Legal Department must ensure compliance with the law and the principles of proportionality and necessity in all activities of the Intelligence Service. Simultaneously, it is tasked with defending the interests of the institution and to cooperate with the judicial bodies. In cases in which the temporary restriction of fundamental civil rights and freedoms is necessary to protect national security, the Legal Department provides the legal rationale for SRI requests before the judicial bodies. In such circumstances, the external mechanism of legal supervision is provided by the Supreme Court of Cassation and Justice or the Public Prosecutor's Office by the Supreme Court of Cassation and Justice.

b) Parliamentary oversight

The legality of SRI activities is guaranteed by the Constitution through parliamentary control. The Parliament appoints the Director of the SRI on the proposal of the Romanian President. Each year, and furthermore at the request of the Parliament, the

---

[67] *Savu*, Direcţia Generală de Informaţii a Apărării – Present şi Perspective. In: Infosfera, Annul I, nr. 3/2009, p. 15.

[68] *Savu*, Direcţia Generală de Informaţii a Apărării – Present şi Perspective. In: Infosfera, Annul I, nr. 3/2009, p. 16.

Director of the SRI submits reports to the Parliament on the activities of the Intelligence Service. The Parliament has, furthermore, established a Standing Committee of the Senate and the Chamber of Deputies for the parliamentary supervision of the activity of the SRI.

c) Financial oversight

The financial oversight of SRI activities is carried out by an internal as well as an external mechanism: Internally, the SRI has an organ for monitoring and assessing the collection, management, and use of financial resources. Externally, financial oversight is carried out by the Romanian Court of Accounts, the Committee for Parliamentary Oversight of the SRI Activity, and the Ministry of Finance. The Court of Accounts carries out its activities autonomously and audits the annual budget execution accounts of the SRI. Finally, the Supreme Council of National Defense approves the annual budgetary costs for operational expenses of the Intelligence Service.

D. Interaction between intelligence services and law enforcement

Despite the separation rule, law enforcement agencies cooperate with the intelligence community. To a certain extent, this is permissible and allowed.

According to Art. 24a) of Law No. 51/1991 on National Security, all state bodies, including the prosecutor's offices, have the obligation to allow such bodies in charge of national security access to the data they hold, if such data concerns national security. By national security, Law no. 51/1991 mentions among other things the security of the legal status of Romania, its social, economic and political stability necessary for the existence and the development of Romania as a sovereign, unified, independent and indivisible state as well as the security of the maintenance of law and the exercise of freedoms and fundamental human rights.[69] National security thus defined is a prerequisite for the maintenance of the rule of law and the unimpeded exercise of human rights.[70] Pursuant to Law No. 51/1991, national security is achieved through situational awareness, prevention and elimination of internal or external threats against the above-mentioned values[71] and in accordance with the laws in force

---

[69] Art. 1 Law No. 51/1991.

[70] *Ungureanu*, Usage of technical surveillance measures in countering threats regarding national security – Comparison between use of technical surveillance measures in criminal procedures and national security threats. In: Journal of Criminal Investigations 1/2015, p. 75.

[71] See Art. 2 Law No. 51/1991. The threats to national security are defined in Art. 3 Law No. 51/1991 as plans or activities against the state's sovereignty, unity, independence or indivisibility. Furthermore, all kinds of activities that provoke *inter alia* war or civil war, military occupation, treason, armed activities against the State, espionage, sabotage,

and obligations deriving from international conventions and protocols for the protection of human rights, which Romania is bound by.[72] Law No. 51/1991 thus constitutes a cooperation between the law enforcement agencies and the intelligence community to a certain extent for the specific purpose of protecting national security.

In spring 2018 – under political pressure[73] – the SRI declassified a secret Cooperation Protocol (*Protocol de Cooperare*[74]) signed in 2009 between the SRI and the Public Ministry – represented by the General Prosecutor's Office – according to which the SRI and prosecution bodies, including the National Anticorruption Directorate (*Direcţia Naţională Anticorupţie, DNA*), have been working together for years.[75] Both institutions had arranged collaboration in the activity of evaluating information in the field of preventing and combating crimes against national security, terrorism, crimes constituting a threat to national security and other serious crimes, in accordance with the law.[76]

To ensure the best possible cooperation between the two institutions, they set up a joint working group, a so-called operational group, to work together according to an action plan in mixed teams of prosecutors and secret service agents. They set up an information system to ensure operational communication, enabling the exchange of information, data, documents and materials among them.[77] Pursuant to the Cooperation Protocol, the exchange of information, data, documents and materials had to be done on principle by prosecutors and officers especially tasked for this, with the approval of the SRI and the head of the respective structure or unit within the prosecutor's office. In exceptional cases, the exchange of information could be performed at an executive level. Prosecutors and secret service agents furthermore took part in

---

activities of a fascist, extremist or terrorist nature, theft of munitions, explosives, toxic or biological substances as well as the creation of or assistance of a terrorist group.

72 See Art. 5 Law No. 51/1991.

73 In 2018 justice minister Tudorel Toader and prime minister Viorica Dăncilă asked for the declassification of the Cooperation Protocols between the SRI and other state institutions.

74 Declassified Cooperation Protocol available at http://media.hotnews.ro/media_server1/document-2018-03-30-22371514-0-protocol-cooperare-parchetul-general-sri.pdf (last visited January 2020). The declassified Cooperation Protocol of 2009 was not the first of this kind. There have been other Cooperation Protocols signed between the SRI and the General Prosecutor's Office between 2003 and 2005. Once the Cooperation Protocol of 2009 came into force, previous protocols ceased to be applicable.

75 There are 64 other collaboration protocols between the SRI and various state institutions according to the chairman of the Parliamentary Committee overseeing the Romanian Intelligence Service (SRI).

See *Radio România Internaţional*, 04.04.2018, available at https://www.rri.ro/en_gb/protocol_between_sri_and_general_prosecutors_office_in_the_spotlight-2579413 (last visited January 2020).

76 Art. 2 Cooperation Protocol 2009.

77 Art. 3 Cooperation Protocol 2009.

joint programs for the formation, specialization, preparation or perfection of their professional activities.[78]

Based on the Protocol, a fruitful cooperation had developed between the SRI and the prosecution bodies. The Protocol opened up the possibility, for instance, for the General Prosecutor's Office to ask the SRI to carry out technical verifications of the identity of the holder of the telephone number proposed for interception and to check the data that emerged throughout the process. The SRI was responsible for recording the communication activities and sending the records to the Prosecutor's Office. The General Prosecutor's Office could also ask the SRI to undertake video technical operations based on authorizations issued by the courts in specific cases through its designated officers. These activities were undertaken with the approval of the Director of the SRI and only in cases of terrorism or acts against national security. For their part, prosecution bodies transmitted, upon request or *ex officio*, information and data to the SRI with a view to preventing or counteracting threats to national security.

In its preamble the Cooperation Protocol of 2009 refers explicitly to the Romanian Constitution, the Code of Criminal Procedure, Law No. 51/1991 on National Security, as well as Law No. 14/1992 on the Organization and Functioning of the SRI and a plethora of other laws relating to the prevention and fight against, for example, organized crime and terrorism. The explicit reference to the constitution and other laws, however, cannot mask the fact that the Protocol was signed as a *secret* document between the Public Ministry – represented by the General Prosecutor's Office as law enforcement agency – and the Romanian Intelligence Service. Through this close cooperation and the loop exchange of information and data, the separation rule has been completely lifted. This was done under the guise of national security. Secret services and their secret methods, however, are to be separated from the coercive measures of the police, who may arrest or conduct searches. Otherwise, this will result in either "police intelligence services" and an "intelligence police force" or a merger into a single "secret police force" that collects information undercover and at the same time is allowed to arrest citizens by force. Those who are exposed to secret measures of the state are not informed about them and cannot defend themselves against them. This constitutes a violation of the right to a fair trial, which is enshrined in Art. 21(3) of the Constitution and in Art. 6 of the European Convention on Human Rights.

The Cooperation Protocol of 2009 led to a legal conflict of a constitutional nature. A conflict of a constitutional nature is assumed if one public authority attributes to itself a competence that is constitutionally assigned to another public authority. According to Art. 146(e) of the Constitution, it is the duty of the Romanian Constitutional Court to solve legal disputes of a constitutional nature between public authorities, at the request of the President of Romania, one of the presidents of the two

[78] Art. 3 Cooperation Protocol 2009.

Chambers, the Prime Minister, or of the president of the Superior Council of the Magistracy. In the present case, it was the Prime Minister who referred the matter to the Romanian Constitutional Court to have it verified whether there was any legal conflict of a constitutional nature between the Public Ministry having signed a secret cooperation protocol from the General Prosecutor's Office and the Romanian Parliament.

According to Art. 1(4) of the Constitution, Romania is based on the principle of separation and balance of powers within the framework of a constitutional democracy. This means that neither a public authority nor the legislator may censor a court decision, nor may a court enact, supplement or modify primary laws (*norme de reglementare primară*). Likewise, administrative acts of the governing bodies of the courts are issued according to the law and for its execution, however, administrative acts do not modify or complete primary laws. Art. 126(2) of the Constitution furthermore stipulates that the jurisdiction of the courts and the judicial procedure are exclusively regulated by law. The adoption of laws, in turn, is the exclusive responsibility of the legislator. Art. 132(1) of the Constitution provides that the prosecutors carry out their activity in accordance with the principles of legality, impartiality, and hierarchical control under the authority of the Minister of Justice. They apply laws that are adopted by the Parliament as sole legislative authority in the country.[79]

In the present case, the Romanian Constitutional Court assumed a constitutional legal conflict between the Public Ministry and the Romanian Parliament. The Court specified that by signing the Cooperation Protocol of 2009, the Public Ministry – represented by the General Prosecutor's Office – created primary law and was hence acting as legislator in violation of Art. 1(4) and Art. 132(2) of the Constitution. The Protocol was the legal basis for the SRI to investigate all areas of crime. The Court stated furthermore that the SRI is not a law enforcement agency and may not issue enforcement orders either independently or in cooperation with prosecutors. The SRI is not allowed to collect or administer evidence for the purpose of introduction into criminal proceedings. The Constitutional Court stated *expressis verbis* that the SRI is not a law enforcement organ and that the Public Ministry cannot cede or transfer parts of its competence under Article 131 of the Constitution[80] to the SRI.

This decision of the Constitutional Court is in line with a leading decision from 2016[81] with regard to intelligence services: Interpreting a provision of the Criminal

---

[79] See Art. 61(1) of the Constitution.

[80] Art. 131 of the Constitution determines: "(1) In the judicial area, the Public Ministry represents the general interests of society and defends the legal order as well as the rights and freedoms of the citizens. (2) The Public Ministry exercises its powers through public prosecutors, organized as public prosecutors' offices, in accordance with the law. (3) Public prosecutor's offices attached to courts of law shall direct and supervise the criminal investigations carried out by the police in accordance with the law."

[81] See decision no. 51/2016 of the Constitutional Court on the exception of unconstitutionality of the provisions of Article 142(1) of the Code of Criminal Procedure, published in

Procedure Code on technical surveillance, the Court concluded that intelligence collected through wiretapping and other technical means is inadmissible as evidence if it was not obtained by the police or a criminal investigation body. The SRI was not considered a criminal investigative body. Before the Court's ruling, the SRI had conducted technical surveillance at the request of the prosecutor's office and other agencies in cases involving not only national security but also corruption, tax evasion, and other crimes.

In conclusion, the Constitutional Court found that the Protocol violated *inter alia* Art. 1(4), Art. 61(1), Art. 126, as well as Art. 131(1) and Art. 132(2) of the Constitution and violated several human rights enshrined in the Constitution, in particular the right to a fair trial according to Art. 21 of the Constitution,[82] the right to individual freedom according to Art. 23 of the Constitution[83] and the right to privacy according to Art. 26 of the Constitution.[84] The Cooperation Protocol of 2009 was declared unconstitutional.

---

the Official Gazette of Romania, Part I, no. 190 of 14 March 2016 and available in English at https://perma.cc/59W8-ZG8S (last visited January 2020).

[82] Art. 21 of the Constitution reads: "(1) Any person may appeal to the organs of justice for the protection of his/her rights, freedoms, and legitimate interests. (2) No law may impede the exercise of this right. (3) All parties shall be entitled to a fair trial and to the resolution of their cases within a reasonable time. (4) Special administrative jurisdictions are elective and free of charge."

[83] Art. 23 of the Constitution reads: "(1) Individual freedom and personal security are inviolable. (2) The search for, detention, or arrest of a person is allowed only in cases specified by law and according to the procedure established by law. (3) The period of detention may not exceed 24 hours. (4) Preventive custody shall be ordered by a judge and only in the course of criminal proceedings. (5) In the course of criminal proceedings, preventive custody may be ordered for a maximum period of 30 days, which may be extended for further periods of up to 30 days each; the overall length of the custody shall not exceed a reasonable term, and not last longer than 180 days. (6) After the lawsuit has begun, the court is obliged, in accordance with the law, to check, on a regular basis and no later than 60 days, the lawfulness and grounds of the preventive custody, and to order at once the release of the defendant if the grounds for the preventive custody no longer exist and if the court finds no new grounds which could justify the extension of the custody. (7) The decisions by a court of law on preventive custody are subject to the legal proceedings provided for by law. (8) The person detained or arrested shall be promptly informed, in the language which he/she understands, of the reasons for his/her detention or arrest and of the charges against him, as soon as possible; he/she will be informed of the charges only in the presence of a counsel chosen by him or appointed by the judge. (9) The release of a detained or arrested person shall be mandatory if the reasons for the detention or arrest have ceased to exist, as well as in other circumstances defined by the law. (10) A person under preventive arrest has the right to ask for provisional release, under judicial control or on bail. (11) A person is considered innocent until the final pronouncement of the sentence. (12) Punishment can be imposed or executed only on a legal basis and in the conditions defined by the law. (13) Sanctions which deprive a person of its freedom can only be based on criminal grounds."

[84] Art. 26 of the Constitution reads: "(1) Public authorities shall respect and protect private and family life. (2) Every person is free to do whatever he/she wants to do, as long as he/she does not violate the rights and freedoms of other persons, public order, or the standards of public morality."

E. Concluding remarks

The systematic acquisition and evaluation of information can be found in all forms of political rule, in dictatorships, oligarchs, monarchies and democracies alike. Although the types and forms of secret service operations have changed greatly throughout history, the basic principles of research, collection and interpretation of secret information have remained similar.[85]

Developments in recent years have shown, however, that the principle of separation has been virtually eliminated by a creeping but constant proximity between police and intelligence services. The Romanian Constitutional Court – as independent oversight body – has put a halt to this development, that is to the policing of the secret services and the clandestine work of the police, and thus to a malicious development. The Constitutional Court takes the constitutional order of functional division in terms of separation of powers and tasks between the police, criminal investigation authorities and intelligence service seriously and puts the latter in its place. The Romanian Constitutional Court has shown itself – once again – to be the guardian of the constitution and the human rights enshrined therein.

List of Abbreviations

CBRN	chemical, biological, radiological and nuclear
CSAT	*Consiliul Suprem de Apărare a Ţării* (Supreme Council of National Defense)
DGIA	Direcţia Generală de Informaţii al Apărării (General Directorate for Defense Intelligence of the Defense Ministry)
DGPI	Direcţia Generală de Protecţie Internă (General Directorate for Internal Security)
JHK	Jahrbuch für Historische Kommunismusforschung
M. Of.	Monitorul Oficial (Official Gazette)
SIE	Serviciul de Informaţii Externe (Foreign Intelligence Service)
SPP	Serviciul de Protecţie şi Pază (Guard and Protection Service)
SRI	Serviciul Român de Informaţii (Romanian Intelligence Service)
SSIAR	*Serviciul Secret al Armatei Române* (Secret Service of the Romanian Army)
STS	*Serviciul de Telecomunicaţii Speciale* (Special Telecommunications Service)

[85] See *Beer*, Die Nachrichtendienste in der Habsburger Monarchie. In: Zeitschrift für Polizeiwissenschaft und polizeiliche Praxis (SIAK-Journal), 2007, (3), S. 53 (53–63).

Bibliography

Beer, *Siegfried*, Die Nachrichtendienste in der Habsburger Monarchie. In: Zeitschrift für Polizeiwissenschaft und polizeiliche Praxis (SIAK-Journal), 2007, (3), pp. 53–63.

Bruneau, Thomas/Matei, Florina Cristina (Cris), Intelligence in the developing democracies: The quest for transparancy and effectiveness. In: Loch K. Johnson (ed.), The Oxford Handbook of National Security Intelligence. Oxford 2010, pp. 757–773.

Caparini, Marina, Controlling and Overseeing Intelligence Services in Democratic States. In: Born, Hans/Caparini Marina (eds.), Democratic Control of Intelligence Services – Containing Rogue Elephants. Hampshire, Burlington 2007, pp. 3–24.

Croitoru, Constantin, Rolul direcţiei generale de informaţii a apărării în sprijinul cu informaţii al categoriilor de forţe din armata României. In: Infosfera, Annul I nr. 3/2009, pp. 27–30.

Deletant, Dennis, British clandestine activities in Romania during the Second World War. 2016.

Deletant, Dennis, Ceauşescu and the Securitate – Coercion and Dissent in Romania, 1965–1989. London, New York 2015.

Fuior, Teodora, The Romanian experience of intelligence oversight. In: Leigh, Ian/Njord Wegge (eds.), Intelligence oversight in the twenty-first century – Accountability in a changing world. London, New York 2019, pp. 57–74.

Leigh, Ian/Wegge, Njord, Intelligence and oversight at the outset of the twenty-first century. In: Leigh, Ian/Njord Wegge (eds.), Intelligence oversight in the twenty-first century – Accountability in a changing world. London, New York 2019, pp. 7–24.

Manda, Anton, Evoluţia sistemului de Securitate în România. In: Revista de Investigare a Criminalităţii 1/2016, pp. 594–604.

Matei, Florina Cristiana, Romania's Anti-Terrorism Capabilities: Transformation, Cooperation, Effectiveness. In: Journal of Defense Resources Management, Vol. 3, Issue 1 (4) 2012, pp. 37–54.

Matei, Florina Cristiana, Reconciling Intelligence Effectiveness and Transparency: The Case of Romania. In: Strategic Insights, Vol. VI, Issue 3 (May 2007). Available at http://edocs.nps.edu/npspubs/institutional/newsletters/strategic%20insight/2007/mateiMay07.pdf (last visited January 2020).

Matei, Florina Cristiana, Romania's Intelligence Community: From an Instrument of Dictatorship to Serving Democracy. In: International Journal of Intelligence and Counter-Intelligence, 20, no. 4, 2007, pp. 629–660.

Matei, *Florina Cristiana*, Romania's Transition to Democracy and the Role of the Press in Intelligence Reform. In: Thomas C. Bruneau/Stefan C. Boraz (eds.), Reforming Intelligence: Obstacles to Democratic Control and Effectiveness, University of Texas Press 2007, pp. 219–240.

Rinceanu, Johanna, National characteristics, fundamental principles, and history of criminal law in Romania. In: Ulrich Sieber/Konstanze Jarvers/Emily Silverman (eds.), National Criminal Law in a Comparative Legal Context, vol. 1.5, Introduction to National Systems. Berlin 2018, pp. 191–278.

Savu, Gheorghe, Direcţia Generală de Informaţii a Apărării – Present şi Perspective. In: Infosfera, Annul I nr. 3/2009, pp. 13–16.

Schreier, Fred, The Need for Efficient and Legitimate Intelligence. In: Born, Hans/Caparini Marina (eds.), Democratic Control of Intelligence Services – Containing Rogue Elephants. Hampshire, Burlington 2007, pp. 25–44.

Söller, Carola, Im Spannungsfeld von „nationalen" und „europäischen" Ansprüchen? Eine Betrachtung des Nationalen Rates für das Studium der Securitate-Archive in Rumänien. In: Jahrbuch für historische Kommunismusforschung 2014, pp. 107–123.

Ungureanu, Petre, Usage of technical surveillance measures in countering threats regarding national security – Comparison between use of technical surveillance measures in criminal procedures and national security threats. In: Journal of Criminal Investigations 1/2015, pp. 75–79.

Watts, Larry L., Control and Oversight of Security Intelligence in Romania. In: Born, Hans/Caparini Marina (eds.), Democratic Control of Intelligence Services – Containing Rogue Elephants. Hampshire, Burlington 2007, pp. 47–64.

Wegge, Njord/Wetzling Thorsten, Contemporary and future challenges to effective intelligence oversight. In: Leigh, Ian/Njord Wegge (eds.), Intelligence oversight in the twenty-first century – Accountability in a changing world. London, New York 2019, pp. 25–39.

Verbrechensbekämpfung durch Nachrichtendienste in der Schweiz

Nadine Zurkinden

I. Einleitung

Die nachrichtendienstlichen Tätigkeiten und die Strafverfolgung werden in der Schweiz von unterschiedlichen Behörden auf Ebene der Kantone und des Bundes wahrgenommen (II.) und verfolgen unterschiedliche Zwecke (III.). Die Verbrechensbekämpfung gehört dabei klar zum Aufgabenfeld der Strafverfolgungsbehörden, deren Beweiserhebung durch die Strafprozessordnung Grenzen gesetzt sind. Demgegenüber können die Nachrichtendienste verdachtslos Informationen beschaffen, wobei ihre Informationsbeschaffungsbefugnisse zum Teil über diejenigen der Staatsanwaltschaft hinausgehen (IV.). Dennoch interagieren Nachrichtendienste und Strafverfolgungsbehörden zuweilen miteinander, was die rechtsstaatlich limitierende

Funktion des strafprozessualen Anfangsverdachts gefährdet[1] und die Nachrichtendienste auch zu Verbrechensbekämpfern macht (V.).

II. Organisation der Sicherheitsbehörden im föderalen Staat

Die Schweiz ist ein föderaler Staat bestehend aus 26 Kantonen. Für die innere Sicherheit ihres Kantonsgebiets sind in erster Linie die Kantone selbst verantwortlich (Art. 4 Abs. 1 Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit, BWIS).[2] Auch für die Organisation ihrer kantonalen Nachrichtendienste sind die Kantone zuständig. Jeder Kanton bestimmt eine Behörde, die mit dem Nachrichtendienst des Bundes (Art. 9 Abs. 1 NDG) und dem Bundesamt für Polizei (fedpol, Art. 6 Abs. 1 BWIS) zur Wahrung der inneren und äusseren Sicherheit der Schweiz zusammenarbeitet. Im Kanton Basel-Stadt besteht diese Behörde aus den Mitarbeitenden einer von der Staatsanwaltschaft eingesetzten Fachgruppe der Kriminalpolizei und dem Leitenden Staatsanwalt, dem auch die Leitung dieser Fachgruppe obliegt (§ 2 Abs. 1 BS-BWIS-Verordnung[3]). Die Staatsschutzbehörde des Kantons Basel-Stadt gehört organisatorisch also zur Staatsanwaltschaft des Kantons Basel-Stadt. In anderen Kantonen ist die kantonale Staatsschutzbehörde Teil der Polizei.[4]

Ist die innere Sicherheit der Schweiz betroffen, ist der Nachrichtendienst des Bundes zuständig. Der Nachrichtendienst des Bundes gehört zum Eidgenössischen Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS).[5] Neben dem Nachrichtendienst des Bundes gibt es auf Bundesebene noch den Nachrichtendienst der Armee. Zu ihm gehören alle jene Stabsteile und Truppen der Armee, die nachrichtendienstliche Aufgaben erfüllen.[6] Gemäss Artikel 99 Abs. 1 Militärgesetz besteht die Aufgabe des Nachrichtendienstes der Armee darin, „für die Armee

---

[1] *Ackermann/Vogler*, NZZ 19. März 2015, 23; *Wohlers*, NZZ vom 18.7.2007, 15.

[2] Bundesgesetz vom 21. März 1997 über Massnahmen zur Wahrung der inneren Sicherheit, BWIS, SR 120.

[3] Basel-Städtische Verordnung über den Vollzug des Bundesgesetzes zur Wahrung der inneren Sicherheit vom 21. September 2010, BWIS-Verordnung, SG 123.200.

[4] *Fabbri/Hunkeler*, in: Forum Strafverteidigung (CH), Vereinigung Österreichischer StrafverteidigerInnen (Ö), Initiative Bayerischer Strafverteidigerinnen und Strafverteidiger e.V. (D) sowie Vereinigung Baden-Württembergischer Strafverteidiger e.V. (D) (Hrsg.), Strafverteidigung und Inquisition, S. 35.

[5] Die Schweizer Regierung besteht aus sieben Bundesräten, jeder steht einem Departement vor. Die sieben Departemente sind: das Eidgenössische Finanzdepartement; das Eidgenössische Departement für auswärtige Angelegenheiten; das Eidgenössische Departement des Innern; das Eidgenössische Justiz- und Polizeidepartement; das Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport; das Eidgenössische Departement für Wirtschaft, Bildung und Forschung; das Eidgenössische Departement für Umwelt, Verkehr, Energie und Kommunikation.

[6] Siehe https://www.vtg.admin.ch/de/organisation/kdo-op/mnd.html [Stand 1.7.2021].

bedeutsame Informationen über das Ausland zu beschaffen und auszuwerten, insbesondere im Hinblick auf die Verteidigung des Landes, den Friedensförderungsdienst und den Assistenzdienst im Ausland." Im Folgenden liegt der Fokus nicht auf dem Nachrichtendienst der Armee, sondern auf dem Nachrichtendienst des Bundes.

Auch die Polizei und Strafverfolgungsbehörden sind kantonal organisiert. In komplexen Fällen schwerer Kriminalität koordiniert, analysiert und ermittelt fedpol als Polizei des Bundes und stellt Infrastruktur zur Verfügung.[7] Die Bundesanwaltschaft ermittelt nur bei Straftaten, die gemäss Artikeln 23 und 24 StPO[8] oder besonderen Bundesgesetzen der Bundesgerichtsbarkeit unterstehen. Darunter fallen etwa die Beteiligung an oder Unterstützung einer kriminellen Organisation oder die Finanzierung des Terrorismus, wenn die Taten entweder zu einem wesentlichen Teil im Ausland begangen worden sind oder wenn sie in mehreren Kantonen begangen worden sind und dabei kein eindeutiger Schwerpunkt in einem Kanton besteht (Art. 24 Abs. 1 StPO).

III. Sicherheitsbehördliche Aufgabenfelder

In der Schweiz besteht eine funktionale Aufteilung der Aufgabenfelder zwischen Nachrichtendiensten, Polizei und Strafverfolgungsbehörden. Der Nachrichtendienst ist dabei vorrangig präventiv ausgerichtet (A.1.), die Polizei wird sowohl zur Gefahrenabwehr als auch gerichtspolizeilich tätig (B.1), die Staatsanwaltschaft ist eine reine Strafverfolgungsbehörde und somit in erster Linie repressiv tätig (C.1). Aus den verschiedenen Aufgabenfeldern ergibt sich auch die Tätigkeitsschwelle bzw. die Verdachtsschwelle, die zum Tätigwerden erreicht werden muss (A.2; B.2; C.2).

A. Nachrichtendienste

1. Aufgaben

Die Aufgaben des Nachrichtendienstes des Bundes sind im Nachrichtendienstgesetz (NDG)[9] geregelt. Das Gesetz regelt den Schutz wichtiger Landesinteressen und bezweckt: a. zur Sicherung der demokratischen und rechtsstaatlichen Grundlagen der Schweiz und zum Schutz der Freiheitsrechte ihrer Bevölkerung beizutragen; b. die Sicherheit der Bevölkerung der Schweiz sowie der Schweizerinnen und

---

[7] Siehe https://www.fedpol.admin.ch/fedpol/de/home/fedpol/fedpol.html [Stand 1.7.2021].

[8] Schweizerische Strafprozessordnung vom 5. Oktober 2007 (Strafprozessordnung), SR 312.0.

[9] Bundesgesetz vom 25. September 2015 über den Nachrichtendienst (Nachrichtendienstgesetz, NDG), SR 121.

Schweizer im Ausland zu erhöhen; c. die Handlungsfähigkeit der Schweiz zu unterstützen; d. zur Wahrung internationaler Sicherheitsinteressen beizutragen (Art. 2 NDG).

Im Falle einer schweren und unmittelbaren Bedrohung kann der Nachrichtendienst darüber hinaus zum Schutz der verfassungsrechtlichen Grundordnung der Schweiz, zur Unterstützung der schweizerischen Aussenpolitik sowie zum Schutz des Werk-, Wirtschafts- und Finanzplatzes Schweiz eingesetzt werden (Art. 3 NDG). Dabei dürfte es regelmässig um die Auslandaufklärung gehen.[10]

Der Nachrichtendienst hat primär eine beobachtende Funktion: Er beschafft und bearbeitet Informationen, um Bedrohungen der inneren und äusseren Sicherheit der Schweiz frühzeitig zu erkennen und zu verhindern.[11] Es geht dabei um Bedrohungen durch Terrorismus, Spionage, Verbreitung von Massenvernichtungswaffen, Cyberangriffe auf kritische Infrastrukturen sowie gewalttätigen Extremismus (Art. 6 Abs. 1 lit. a NDG). Ausserdem beurteilt der Nachrichtendienst die Bedrohungslage, trifft und plant entsprechende Massnahmen und alarmiert bei Bedarf die zuständigen staatlichen Stellen (Art. 6 Abs. 2 NDG).[12]

Nicht zu seinen Aufgaben gehören die neutrale Aufklärung strafbaren Verhaltens[13] oder klassische Polizeiaufgaben, wie das Anhalten einer Person. Der NDB kann zwar Personen anhalten lassen, die Anhaltung muss aber durch Angehörige eines kantonalen Polizeikorps erfolgen (Art. 24 Abs. l und 2 NDG).[14]

2. Tätigkeitsschwelle – Qualität der Verdachtsmomente

Im Gegensatz zu den Strafverfolgungsbehörden, die erst tätig werden dürfen, wenn sie einen Anfangsverdacht haben, dass eine Straftat begangen wurde (etwa auf Grund einer Strafanzeige),[15] darf der Nachrichtendienst des Bundes bereits vor Vorliegen eines Tatverdachts Informationen beschaffen. Für genehmigungsfreie Informationsbeschaffungsmassnahmen ist nicht einmal vorausgesetzt, dass eine „konkrete Bedrohung" gemäss Art. 19 NDG[16] vorliegt. Vielmehr geht es bei der Informationsbeschaffung um die Suche nach der Bedrohung.[17]

---

[10] *Isenring/Quiblier*, Sicherheit & Recht, 3/2017, 128 f.

[11] *Ackermann/Vogler*, NZZ 19. März 2015, 23.

[12] *Isenring/Quiblier*, Sicherheit & Recht, 3/2017, 129. Siehe auch: https://www.vbs.admin.ch/de/vbs/organisation/verwaltungseinheiten/nachrichtendienst.html [Stand 1.7.2021].

[13] *Ackermann/Vogler*, NZZ 19. März 2015, 23.

[14] *Gertsch/Stähli*, in: Kiener/Bühler/Schindler (Hrsg.), Sicherheits- und Ordnungsrecht des Bundes, Rn. 81, die darauf hinweisen, dass hingegen gemäss Art. 26 Abs. l lit. e NDG Durchsuchungen von Räumlichkeiten, Fahrzeugen und Behältnissen durch den Nachrichtendienst nach vorgängigem Genehmigungsverfahren selber durchgeführt werden dürfen.

[15] *Wohlers*, ZStrR 2017, 469.

[16] Siehe unten IV.B.

[17] *Ackermann/Vogler*, in: Ackermann/Hilf, TOP SECRET Geheimnisschutz und Spionage, S. 169.

Erst für genehmigungspflichtige Informationsbeschaffungsmassnahmen muss eine konkrete Bedrohung bestehen. Die Kabelaufklärung ist wiederum (obwohl genehmigungspflichtig) möglich, ohne dass eine konkrete Bedrohung vorliegt.[18]

B. Polizei

1. Aufgaben

Die Polizei hat ein sehr breites Aufgabenspektrum, das unterschiedlichen Regelwerken untersteht. So wird sie einerseits präventiv tätig und wehrt Gefahren für die öffentliche Ordnung und Sicherheit ab und beseitigt Störungen.[19] Diese Tätigkeit wird primär im kantonalen Polizeirecht geregelt.[20] Schwere Eingriffe in individuelle Rechtsgüter setzen dabei hohe Gefahrstufen voraus. So setzt etwa der polizeiliche Schusswaffengebrauch voraus, dass Personen für andere Personen eine *unmittelbar drohende Gefahr* an Leib und Leben darstellen (§ 48 Gesetz betreffend die Kantonspolizei des Kantons Basel-Stadt, PolG BS). Die Polizei wird aber auch gerichtspolizeilich zur Ermittlung von Straftaten also repressiv tätig. Die Übergänge sind jeweils fliessend.[21] So sichert etwa die Polizei nach einem Unfall die Unfallstelle, regelt den Verkehr und verhindert dadurch Folgeunfälle. Gleichzeitig sichert sie aber auch die Unfallspuren für die Strafverfolgung und führt erste polizeiliche Befragungen durch. Sie wird somit auch repressiv als Strafverfolgungsbehörde (Art. 12 StPO) tätig und wird in dieser Funktion auch als gerichtliche Polizei bezeichnet.[22]

Im Vorfeld der Strafverfolgung kann die Polizei aber auch proaktiv tätig werden Diese Tätigkeiten im gerichtspolizeilichen Vorfeld dienen aber nicht dazu Bedrohungen der inneren und äusseren Sicherheit der Schweiz zu erkennen und zu verhindern. Vielmehr geht es darum, *Straftaten* aufzudecken, die noch nicht bekannt sind bzw. nicht angezeigt wurden. So bezweckt etwa die verdeckte Fahndung, „mit Angehörigen der Polizei, deren wahre Identität und Funktion nicht erkennbar ist, im Rahmen kurzer Einsätze ohne Verwendung einer Legende die Vorbereitung von Verbrechen und Vergehen zu erkennen oder Straftaten zu verhindern“ (§ 33a Abs. 1 PolG BS). Etwa Straftaten im Zusammenhang mit organisierter Kriminalität. Die operative Arbeit der Polizei im gerichtspolizeilichen Vorfeld mündet schliesslich in der Strafverfolgung, die in der Zuständigkeit der Strafverfolgungsbehörden liegt.[23]

---

[18] Siehe ausführlich zu den unterschiedlichen Informationsbeschaffungsmassnahmen unten IV.B.

[19] Vgl. statt vieler *Rauber*, Rechtliche Grundlagen, S. 49.

[20] BSK StPO-*Uster*, Art. 15 N 2.

[21] BSK StPO-*Uster*, Art. 15 N 4.

[22] *Reinhard*, Polizeirecht, S. 35.

[23] *Ackermann/Vogler*, in: Ackermann/Hilf, TOP SECRET Geheimnisschutz und Spionage, S. 166–169.

2. Tätigkeitsschwelle – Qualität der Verdachtsmomente

Je nach polizeilicher Tätigkeit wird die Polizei früh tätig (wenn nicht in individuelle Rechtsgüter eingegriffen wird kann sie auch tätig werden, ohne dass konkrete Gefahren vorliegen) und oft in Bereichen, die keine strafrechtliche Relevanz haben. So unterrichtet die Polizei beispielsweise Kinder über das richtige Verhalten im Verkehr[24] oder prüft Baustellen hinsichtlich Verkehrssicherheit und Verkehrsfluss[25]. Im gerichtspolizeilichen Vorfeld wird sie aufgrund eines vagen Verdachts tätig, dass in dem zu überprüfenden Bereich strafbare Handlungen begangen werden oder worden sein könnten. Dieser vage Verdacht ist noch kein hinreichender strafprozessualer Anfangsverdacht, er ist aber auch kein nachrichtendienstlicher Bedrohungsverdacht. Vielmehr soll mit der Vorabklärung festgestellt werden, ob möglicherweise ein Anfangsverdacht besteht. Problematisch ist dabei, dass die Grenze zwischen Ermittlungen im gerichtspolizeilichen Vorfeld und einem Anfangsverdacht, der für ein strafprozessuales Vorverfahren vorausgesetzt wird (Art. 7 Abs. 1; Art. 299 Abs. 2 StPO) schwierig zu erkennen ist.[26] Dem wird aber dadurch Rechnung getragen, dass im gerichtspolizeilichen Vorfeld keine Zwangsmassnahmen eingesetzt werden dürfen.[27]

C. Staatsanwaltschaft

1. Aufgaben

Die Staatsanwaltschaft ist eine reine Strafverfolgungsbehörde (Art. 12 StPO). Die Strafverfolgung bezweckt die Verfolgung und Beurteilung von Straftaten durch die Strafbehörden (Art. 1 StPO). Strafverfolgungsbehörden werden somit repressiv tätig. Nichtsdestotrotz hat die Staatsanwaltschaft einen gesetzlichen Auftrag zur neutralen Aufklärung strafbaren Verhaltens, denn sie hat, wie alle Strafbehörden,[28] belastende und entlastende Beweise gleichermassen zu erheben (Art. 6 Abs. 2 StPO).[29] Sie leitet das Vorverfahren, verfolgt Straftaten im Rahmen der Untersuchung, erhebt gegebenenfalls Anklage und vertritt die Anklage (Art. 16 Abs. 2 StPO).

---

[24] Siehe z.B. https://www.polizei.bs.ch/praevention/verkehrspraevention.html [Stand 1.7.2021].

[25] Siehe z.B. https://www.polizei.bs.ch/verkehr/verkehrssicherheit.html [Stand 1.7.2021].

[26] *Zurkinden*, Joint Investigation Teams, S. 92–95 m.w.Nw.

[27] *Wohlers*, ZStrR 2017, 469.

[28] Strafbehörden ist der Oberbegriff für Strafverfolgungsbehörden und Gerichte. Siehe StPO, 2. Titel.

[29] *Ackermann/Vogler*, NZZ 19. März 2015, 23.

2. Tätigkeitsschwelle – Qualität der Verdachtsmomente

Die Strafverfolgung kann nur aufgrund eines Verdachts, es sei eine Straftat begangen worden, aufgenommen werden (Art. 299 Abs. 2 StPO). Man spricht dabei vom Anfangsverdacht.[30] Dabei reicht es, dass „Anzeichen auf eine strafbare Handlung hindeuten, also eine gewisse Wahrscheinlichkeit strafbaren Verhaltens besteht."[31] Der Anfangsverdacht bildet damit eine wichtige Schranke gegen ungerechtfertigte Strafverfolgung, denn verdachtslose Ermittlungen sind den Strafverfolgungsbehörden verboten.[32]

Zwangsmassnahmen (z.B. Hausdurchsuchung, Beschlagnahme) erfordern den erhöhten Verdachtsgrad des sogenannten hinreichenden Tatverdachts (Art. 197 Abs. 1 lit. b StPO). Die StPO definiert nicht, was hinreichend bedeutet. Das Bundesgericht führt dazu aus: „Hinweise auf eine strafbare Handlung müssen erheblich und konkreter Natur sein, um einen hinreichenden Tatverdacht begründen zu können" (BGE 141 IV 87 ff., 90 E. 1.3.1). Mit zunehmender Schwere des Grundrechtseingriffs steigen die Anforderungen an den Verdachtsgrad. So sind etwa die Untersuchungshaft (Art. 221 Abs. 1 StPO) und die Überwachung des Post- und Fernmeldeverkehrs (Art. 269 Abs. 1 StPO) nur möglich, wenn ein dringender Tatverdacht vorliegt.[33]

IV. Nachrichtendienste als Verbrechensbekämpfer?

A. Strafverfolgungsrelevante Aufgabenfelder der Nachrichtendienste

Der Nachrichtendienst des Bundes beschafft und bearbeitet Informationen um Bedrohungen der inneren und äusseren Sicherheit zu erkennen und zu verhindern, die ausgehen von „1. Terrorismus, 2. verbotenem Nachrichtendienst, 3. der Weiterverbreitung nuklearer, biologischer oder chemischer Waffen, einschliesslich ihrer Trägersysteme, sowie aller zur Herstellung dieser Waffen notwendigen zivil und militärisch verwendbaren Güter und Technologien (NBC-Proliferation) oder dem illegalen Handel mit radioaktiven Substanzen, Kriegsmaterial und anderen Rüstungsgütern, 4. Angriffen auf Informations-, Kommunikations-, Energie-, Transport- und weitere Infrastrukturen, die für das Funktionieren von Gesellschaft, Wirtschaft und Staat unerlässlich sind (kritische Infrastrukturen), 5. gewalttätigem Extremismus." (Art. 6 Abs. 1 lit. a NDG).

---

30 BSK StPO-*Riedo/Boner*, Art. 299 N 13 und 15.

31 BSK StPO-*Riedo/Boner*, Art. 300 N 5.

32 *Von Hahn*, forumpoenale 3/2016, 150 m.w.Nw.

33 BSK StPO-*Weber*, Art. 197 N 8.

Bei diesen Aufgabenfeldern handelt es sich gleichzeitig um Kriminalitätsfelder. Die Gefahr einer Überlappung mit der Tätigkeit der Strafverfolgungsbehörden besteht vor allem bei Kriminalitätsfeldern, deren Strafbarkeit vom Gesetzgeber noch vor den strafbaren Beginn des Versuchs vorgelagert wurde. Dies ist etwa der Fall bei Vorbereitungshandlungen zu vorsätzlicher Tötung, Mord, schwerer Körperverletzung, Verstümmelung weiblicher Genitalien, Raub, Freiheitsberaubung und Entführung, Geiselnahme, Verschwindenlassen, Brandstiftung, Völkermord, Verbrechen gegen die Menschlichkeit und Kriegsverbrechen (Art. 260bis Abs. 1 StGB). Vorverlagert ist die Strafbarkeit auch im Zusammenhang mit kriminellen Organisationen: strafbar macht sich bereits, wer sich an einer solche Organisation beteiligt oder sie unterstützt (Art. 260ter StGB). Weitere Beispiele der Vorverlagerung der Strafbarkeit sind die Gefährdung der öffentlichen Sicherheit mit Waffen (Art. 260^{quater} StGB) und die Finanzierung des Terrorismus (Art. 260^{quinquies} StGB).[34] Aus rechtstaatlicher Sicht spitzt sich die Überschneidungsgefahr noch dadurch zu, dass der Nachrichtendienst des Bundes seit dem 1. September 2017 neue und sehr weitgehende Befugnisse erhalten hat.

B. Neue Befugnisse für eine effektive nachrichtendienstliche Verbrechensbekämpfung

1. Früher: beschränkte Befugnisse aufgrund der Fichenaffäre

Nachdem 1989 eine parlamentarische Untersuchungskommission aufdeckte, dass hunderttausende Bürger in der Schweiz überwacht wurden, weil sie als „subversiv" galten (sogenannte Fichenaffäre), [35] ergriff die Schweizer Regierung (Bundesrat) verschiedene Sofortmassnahmen. Sie erliess beispielsweise Richtlinien und erstellte eine Liste, in welcher Vorgänge, Personen und Organisationen aufgeführt wurden, über die keine Informationen mehr bearbeitete werden durften.[36] Das Bundesgesetz vom 21. März 1997 über Massnahmen zur Wahrung der inneren Sicherheit, das in der Folge am 1. Juli 1998 in Kraft trat, beschränkte die Befugnisse des präventiven zivilen Staatsschutzes. Nicht allgemein zugängliche Orte (z.B. Hotelzimmer) waren generell jeder Gefährdungsabklärung entzogen. Abklärungen über staatsschutz-

---

[34] *Isenring/Quiblier*, Sicherheit & Recht, 3/2017, 130 m.w.Nw.; *Pieth*, in: Forum Strafverteidigung (CH), Vereinigung Österreichischer StrafverteidigerInnen (Ö), Initiative Bayerischer Strafverteidigerinnen und Strafverteidiger e.V. (D) sowie Vereinigung Baden-Württembergischer Strafverteidiger e.V. (D) (Hrsg.), Strafverteidigung und Inquisition, S. 18.

[35] Siehe etwa *Kreis*, Staatsschutz in der Schweiz, *passim*; *Bucherli*, NZZ 13.7.2009; *Clavadetscher*, Luzerner Zeitung; Videos zum Thema: https://www.srf.ch/sendungen/myschool/die-fichenaffaere [Stand 1.7.2021].

[36] Botschaft zum Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit und zur Volksinitiative «S.O.S. Schweiz ohne Schnüffelpolizei» vom 7. März 1994, BBl 1994 II 1128.

relevante Bedrohungen endeten grundsätzlich an der «Tür zum privaten Raum».[37] So war etwa auch die Überwachung des Telefonverkehrs potenzieller Terroristen nicht erlaubt, falls es zwar einen Verdacht gab, aber gegen die betroffene Person kein Strafverfahren eingeleitet wurde.[38]

2. Neue Befugnisse seit 1. September 2017

Nicht einmal zwei Jahrzehnte nach Inkrafttreten des BWIS reichte nach Auffassung der Schweizer Regierung das „Instrumentarium […] nicht mehr aus, um die präventiven Aufgaben des NDB angesichts der immer aggressiveren Akteure, die die innere oder die äussere Sicherheit der Schweiz bedrohen und angesichts der komplexeren Bedrohungsformen weiterhin wahrzunehmen."[39] Es wurde deshalb ein neues Nachrichtendienstgesetz erarbeitet, gegen das erfolglos das Referendum ergriffen wurde. Das neue Nachrichtendienstgesetz wurde von allen Kantonen und mit 65,5% Ja-Stimmen angenommen.[40] Am 1. September 2017 ist es zusammen mit drei dazugehörigen Verordnungen[41] in Kraft getreten.[42]

Seit Inkrafttreten des NDG kann der NDB zur Erfüllung seiner Aufgaben Informationen aus öffentlich und nicht öffentlich zugänglichen Informationsquellen (Art. 5 Abs. 1 NDG) beschaffen. Der Nachrichtendienst hat dabei nicht nur die Befugnis, allgemeine Informationen zu sammeln, sondern kann auch verdeckt Informationen über bestimmte Personen beschaffen (Art. 5 Abs. 4 NDG). Etwa, wenn konkrete Anhaltspunkte vorliegen, dass eine Person terroristische, verbotene nachrichtendienstliche oder gewalttätig-extremistische Tätigkeiten vorbereitet oder durchführt (Art. 5 Abs. 6 NDG).

3. Weitgehende Informationsbeschaffungsbefugnisse

Das NDG ermöglicht dem Nachrichtendienst des Bundes zudem Informationsbeschaffungsmassnahmen, die teilweise sogar über die Zwangsmassnahmen hinaus-

---

[37] Botschaft zur Änderung des Bundesgesetzes über Massnahmen zur Wahrung der inneren Sicherheit (BWIS)(Besondere Mittel der Informationsbeschaffung) vom 15. Juni 2007, BBl 2007, 5058.

[38] *Gerny*, NZZ 18.8.2016.

[39] Botschaft zum Nachrichtendienstgesetz vom 19. Februar 2014, BBl 2014, 2107.

[40] Bundeskanzlei, Vorlage Nr. 607 Bundesgesetz vom 25.09.2015 über den Nachrichtendienst (online abrufbar: https://www.bk.admin.ch/ch/d/pore/va/20160925/can607.html [Stand 1.7.2021]).

[41] Verordnung vom 16. August 2017 über den Nachrichtendienst (Nachrichtendienstverordnung, NDV), SR 121.1; Verordnung vom 16. August 2017 über die Informations- und Speichersysteme des Nachrichtendienstes des Bundes (VIS-NDB), SR 121.2; Verordnung vom 16. August 2017 über die Aufsicht über die nachrichtendienstlichen Tätigkeiten (VAND), SR 121.3.

[42] *Isenring/Quiblier*, Sicherheit & Recht, 3/2017, 127.

gehen, welche die Strafverfolgungsbehörden einsetzen dürfen.[43] Das NDG unterscheidet dabei zwischen genehmigungsfreien und genehmigungspflichtigen Informationsbeschaffungsmassnahmen (Art. 5 Abs. 2 NDG). Einem erleichterten Genehmigungsverfahren unterstehen dabei die separat geregelte Beschaffung von Informationen über Vorgänge im Ausland (Art. 36 ff. NDG) und die Kabelaufklärung (Art. 39 ff. NDG).[44]

a) Genehmigungsfreie Informationsbeschaffungsmassnahmen

Genehmigungsfrei und ohne zeitliche Beschränkung kann der Nachrichtendienst Informationen aus öffentlichen Quellen (Art. 13 NDG, z.B. aus öffentlich zugänglichen Medien – etwa öffentlichen Einträgen in sozialen Netzwerken wie Facebook, LinkedIn, Twitter, Instagram – und behördlichen Registern) beschaffen sowie öffentliche und allgemein zugängliche Orte (z.B. Flughäfen, öffentliche Plätze) beobachten (Art. 14 NDG).[45] Der Nachrichtendienst kann bei der Informationsbeschaffung auch von sogenannten menschlichen Quellen unterstützt werden, die vom NDB entschädigt werden können und für deren Schutz der NDB die notwendigen Massnahmen trifft (Art. 15 NDG). Solche menschlichen Quellen sind Personen, die beispielsweise Zugang zu terroristischen Gruppierungen haben und die aus eigener Motivation oder auf Anfrage des NDB bereit dazu sind, Informationen an den NDB weiterzugeben. Möglich ist auch, dass die menschlichen Quellen ohne ihr Wissen Informationen an den Nachrichtendienst liefern.[46] Dass menschliche Quellen vom NDB entschädigt werden können, könnte allerdings ein Anreiz für Fehlinformation sein.[47]

Ausserdem kann der Nachrichtendienst genehmigungsfrei Personen und Fahrzeuge im Polizeifahndungssystem der Schweiz (RIPOL[48]) sowie im nationalen Teil des Schengener Informationssystems (N-SIS) ausschreiben lassen, um so die Bewegungen von bestimmten Zielpersonen festzustellen, [49] wenn begründete Anhaltspunkte vorliegen, dass von einer Person eine konkrete Bedrohung für die innere oder äussere Sicherheit der Schweiz ausgeht oder wenn es gemäss Bundesratsbeschluss (Art. 3 i.V.m. Art. 70 NDG) zur Wahrung weiterer wichtiger Landesinteressen gemäss Art. 3 NDG notwendig ist, den Aufenthalt einer Person festzustellen.[50] Ähnliches gilt für die Ausschreibung von Fahrzeugen: Sie können ausgeschrieben werden,

---

43 *Ackermann/Vogler*, NZZ 19. März 2015, 23.

44 *Isenring/Quiblier*, Sicherheit & Recht, 3/2017, 132.

45 *Isenring/Quiblier*, Sicherheit & Recht, 3/2017, 132 m.w.Nw.

46 Botschaft zum Nachrichtendienstgesetz vom 19. Februar 2014, BBl 2014, 2151 f.

47 *Isenring/Quiblier*, Sicherheit & Recht 3/2017, 133.

48 Diese Abkürzung steht für „Recherches informatisées de police".

49 Botschaft zum Nachrichtendienstgesetz vom 19. Februar 2014, BBl 2014, 2153.

50 *Isenring/Quiblier*, Sicherheit & Recht 3/2017, 133.

wenn sie für eine Bedrohung der Sicherheit der Schweiz benutzt werden; wenn sie von einer Person, von der eine Bedrohung ausgeht, benutzt werden; oder wenn es zur Wahrung weiterer wichtiger Landesinteressen gemäss Art. 3 NDG notwendig ist, den Aufenthalt eines Fahrzeugs festzustellen.

Fahrzeuge von Drittpersonen, die einem Berufsgeheimnis unterstehen (z.B. Geistliche, Rechtsanwälte, Ärzte, usw.), dürfen laut Art. 16 Abs. 3 NDG nicht überwacht werden, ausser es liegen begründete Anhaltspunkte vor, dass von dieser Person selber eine konkrete Bedrohung für die Sicherheit der Schweiz ausgeht.[51]

b) Genehmigungspflichtige Informationsbeschaffungsmassnahmen

Die genehmigungspflichtigen Informationsbeschaffungsmassnahmen werden in Art. 26 NDG aufgezählt. Dazu gehören die Überwachung des Post- und Fernmeldeverkehrs, der Einsatz von Ortungs- und Überwachungsgeräten, das Eindringen in Computersysteme oder -netzwerke (Hacking), das Durchsuchen von Sachen (nicht jedoch das Durchsuchen von Personen). Alle diese Massnahmen werden verdeckt durchgeführt (Art. 26 Abs. 2 NDG). Berufsgeheimnisse darf der NDB nicht erfahren, ausser die vom Berufsgeheimnis erfassten Informationen hängen mit dem Grund zusammen, aus welchem die Überwachung angeordnet wurde (Art. 23 NDV).

Der NDB kann gemäss Art. 27 NDG eine genehmigungspflichtige Informationsbeschaffungsmassnahme nur anordnen, wenn folgende Voraussetzungen erfüllt sind:

Zunächst muss eine konkrete Bedrohung vorliegen oder der die Wahrung weiterer wichtiger Landesinteressen müssen die Informationsbeschaffungsmassnahme erforderlich machen. Eine konkrete Bedrohung liegt gemäss Art. 19 Abs. 2 NDG i.V.m. Art. 27 NDG vor, wenn ein bedeutendes Rechtsgut wie Leib und Leben oder Freiheit von Personen oder Bestand und Funktionieren des Staates betroffen ist und die Bedrohung ausgeht von Terrorismus, Spionage, Verbreitung von Massenvernichtungswaffen oder Angriffen auf kritische Infrastrukturen.

Ausserdem muss die Anordnung der Informationsbeschaffungsmassnahme verhältnismässig sein:[52] Erstens muss die Schwere der Bedrohung die Massnahme rechtfertigen. Zweitens müssen die nachrichtendienstlichen Abklärungen bisher erfolglos gewesen sein oder sie müssen aussichtslos oder ohne die genehmigungspflichtige Massnahme unverhältnismässig erschwert sein.

Sie bedürfen ausserdem der *Genehmigung* des Präsidenten oder der Präsidentin der zuständigen Abteilung des Bundesverwaltungsgerichts (als Einzelrichter*in, Art. 29 Abs. 2 NDG) sowie der Freigabe durch die Vorsteherin[53] des VBS. Die Genehmigung wird für drei Monate erteilt, kann aber verlängert werden (Art. 29 Abs.

---

[51] *Isenring/Quiblier*, Sicherheit & Recht 3/2017, 134.

[52] *Isenring/Quiblier*, Sicherheit & Recht 3/2017, 135.

[53] Zurzeit ist das Viola Amherd.

6 NDG). Über die Freigabe entscheidet die Vorsteherin des VBS nach vorheriger (schriftlicher) Konsultation des Vorstehers des Eidgenössischen Departements für auswärtige Angelegenheiten (EDA)[54] und der Vorsteherin des Eidgenössischen Justiz- und Polizeidepartement (EJPD)[55]. Fälle von besonderer Bedeutung können dem Bundesrat vorgelegt werden (Art. 30 NDG). Bei Dringlichkeit kann der Direktor des NDB[56] die Informationsbeschaffungsmassnahme anordnen. Er muss aber umgehend die Vorsteherin des VBS orientieren und einen Genehmigungsantrag beim Bundesverwaltungsgericht einreichen. Die Vorsteherin des VBS kann die Beschaffungsmassnahme sofort beenden. Das Gericht entscheidet innert drei Arbeitstagen über die Genehmigung der Informationsbeschaffungsmassnahme. Über die Freigabe entscheidet dann wiederum die Vorsteherin des VBS nach vorheriger Konsultation des Vorstehers des EDA und der Vorsteherin des EJPD (Art. 31 NGD).

Kritiker befürchten, dass die Genehmigung durch einen Einzelrichter/eine Einzelrichterin eher erteilt wird, als wenn ein Gremium von mindestens drei Richtern hätte entscheiden müssen. Ausserdem führe das mehrstufige Prozedere von richterlicher Genehmigung und Freigabe durch das VBS zu einer Verantwortungsdiffusion zwischen den Entscheidungsträgern.[57] Dagegen monierte der Chef des NDB (Jean-Philippe Gaudin), dass das Genehmigungsverfahren zu aufwendig sei und beantragte und erhielt mehr Mitarbeitende.[58]

c) Beschaffung von Informationen über Vorgänge im Ausland

Werden im Inland Informationen über Vorgänge im Ausland beschafft, gilt grundsätzlich dasselbe zweistufige Prozedere von einzelrichterlicher Genehmigung und Freigabe durch das VBS (Art. 36 Abs. 2 NDG). Keiner richterlichen Genehmigung bedarf das Eindringen in Computersysteme und Computernetzwerke im Ausland. Dringt der NDB in diese ein, um dort vorhandene oder von dort aus übermittelte Informationen über Vorgänge im Ausland zu beschaffen, bedarf es nur der Zustimmung der Vorsteherin des VBS, die vorher die Vorsteher des EDA und des EJPD konsultiert. Der Gesamtbundesrat muss jedoch entscheiden, ob der NDB in Computersysteme und -netzwerke im Ausland eindringen darf, um den Zugang zu Informationen zu stören, zu verhindern oder zu verlangsamen, wenn die Computersysteme und -netzwerke für Angriffe auf kritische Infrastrukturen in der Schweiz verwendet werden (Art. 37 NDG).

---

[54] Zurzeit ist das Ignazio Cassis.

[55] Zurzeit ist das Karin Keller-Sutter.

[56] Zurzeit ist das Jean-Philippe Gaudin.

[57] *Isenring/Quiblier*, Sicherheit & Recht 3/2017, 136.

[58] *Meier*, Ruf nach mehr Ressourcen, SRF 19. Oktober 2018.

d) Kabelaufklärung

Das zweistufige Prozedere (einzelrichterliche Genehmigung und Freigabe durch eine politische Instanz) gilt auch für die sogenannte *Kabelaufklärung* (Art. 40 f. NDG). Sie ermöglicht die verdachtsunabhängige Massenüberwachung von grenzüberschreitenden Internetverbindungen und gilt deswegen als „weitaus eingreifendste Neuerung des NDG."[59] Der NDG kann gemäss Art. 39 Abs. 1 das Zentrum für elektronische Operationen der Schweizer Armee (ZEO) beauftragen, Informationen über sicherheitspolitisch bedeutsame Vorgänge im Ausland sowie zur Wahrung weiterer Landesinteressen nach Art. 3 NDG zu beschaffen. Dazu werden Datenströme angezapft und anhand von Stichworten gescannt.[60] Das ZEO darf dem Nachrichtendienst nur Daten weiterleiten, wenn deren Inhalt definierten Suchbegriffen entspricht. „Die Suchbegriffe sind so zu definieren, dass ihre Anwendung möglichst geringe Eingriffe in die Privatsphäre von Personen verursacht. Angaben über schweizerische natürliche oder juristische Personen sind als Suchbegriff nicht zulässig."[61] Ausserdem darf die elektronische Kommunikation nur überwacht werden, wenn sich Sender oder Empfänger im Ausland befinden. Rein schweizerische Kommunikation darf nicht überwacht werden (Art. 39 Abs. 2 NDG).

Die Kabelaufklärung wird trotz dieser Einschränkungen stark kritisiert, da die Überwachung bereits beim Sammeln nicht erst bei der Auswertung von Daten beginne und die Internetnutzung in der Schweiz fast immer auch über Netzwerke im Ausland erfolge, womit der Nachrichtendienst Zugriff auf sämtliche Inhalte elektronischer Kommunikation habe.[62] Die Massenüberwachung erfolgt zudem verdachtsunabhängig und erfasst zwangsläufig auch Personen, die einem Berufsgeheimnis unterstehen. Ausserdem ist der Quellenschutz von Medienschaffenden so nicht mehr vollumfänglich gewährleistet.[63]

---

[59] *Isenring/Quiblier*, Sicherheit & Recht 3/2017, 138.

[60] *Isenring/Quiblier*, Sicherheit & Recht 3/2017, 138 f.

[61] Art. 39 Abs. 3 NDG.

[62] *Steiger*, Neues Nachrichtendienstgesetz in der Schweiz, netzpolitik.org, 12.01.2016. Siehe auch *Steiger*, Sicherheitsesoterik statt Menschenrechte, digma 2015, 136.

[63] *Isenring/Quiblier*, Sicherheit & Recht 3/2017, 139.

V. Interaktion zwischen Nachrichtendiensten und Strafverfolgungsbehörden

A. Interaktion zwischen Nachrichtendiensten und Strafverfolgungsbehörden – im Allgemeinen

In Anbetracht der neuen und weitgehenden Informationsbeschaffungsbefugnissen des NDG gewinnt die Frage, ob und inwiefern sich die Nachrichtendienste von den Strafverfolgungsbehörden trennen lassen, an Bedeutung. Zumal die Dienste wohl durch die neuen Befugnisse über Material verfügen, das auch für die Strafverfolgung relevant sein könnte. In der Schweiz wird diese Fragestellung nur sporadisch angeschnitten. Das in Deutschland in diesem Zusammenhang als regulativ herangezogene Trennungsgebot bietet sich als ein aufschlussreicher Anhaltspunkt auch für die Bewertung der genannten Fragestellung in der Schweiz an. Das Trennungsgebot, das seit dem Ende der Gestapo in Deutschland gilt, wird in der Schweizer Literatur erwähnt.[64] Es ist jedoch nicht ihr primäres Thema. Immerhin ist man sich einig, „dass der NDB kein primärer Zulieferer für die Strafverfolgungsbehörden sein darf."[65] Das Bundesgericht setzt sich jedoch soweit ersichtlich nicht mit dem Trennungsgebot auseinander.[66]

Die Trennung von Nachrichtendienst und Strafverfolgungsbehörden ergibt sich in der Schweiz durch die unterschiedlichen Aufgabenfelder (siehe oben III.). Sie wird auch beim Genehmigungsverfahren eingehalten, indem unterschiedliche Gerichte über Massnahmen entscheiden:[67] Das Zwangsmassnahmengericht entscheidet über Zwangsmassnahmen im Strafverfahren; das Bundesverwaltungsgericht (und die Vorsteherin des VBS) über genehmigungspflichtigen Massnahmen des NDB. Auch organisatorisch sind Nachrichtendienste und Strafverfolgungsbehörden mindestens auf Bundesebene getrennt (siehe oben II.). Das Trennungsgebot sollte allerdings nicht auf seine organisatorische Komponente reduziert werden.

---

[64] *Ackermann/Vogler*, NZZ 19. März 2015, 23; *Fabbri/Hunkeler*, in: Forum Strafverteidigung (CH), Vereinigung Österreichischer StrafverteidigerInnen (Ö), Initiative Bayerischer Strafverteidigerinnen und Strafverteidiger e.V. (D) sowie Vereinigung Baden-Württembergischer Strafverteidiger e.V. (D) (Hrsg.), Strafverteidigung und Inquisition, S. 33.

[65] *Gertsch/Stähli*, in: Kiener/Bühler/Schindler (Hrsg.), Sicherheits- und Ordnungsrecht des Bundes, Rn. 81 mit Verweis auf die Botschaft zum Nachrichtendienstgesetz vom 19. Februar 2014, BBl 2014, 2120. Mit Blick auf die bundesgerichtliche Rechtsprechung zur Beweisverwertung werden jedoch auch Zweifel an der tatsächlichen Geltung eines Trennungsgebots in der Schweiz geäussert (*Roos/Jeker*, forumpoenale 2017, 414). Dazu und zum Informationsaustausch zwischen Nachrichtendienst und Strafverfolgungsbehörde siehe unten V.

[66] Siehe etwa Bundesgericht 6B_57/2015 und 6B_81/2015 vom 27. Januar 2016; *Fabbri/Hunkeler*, in: Forum Strafverteidigung (CH), Vereinigung Österreichischer StrafverteidigerInnen (Ö), Initiative Bayerischer Strafverteidigerinnen und Strafverteidiger e.V. (D) sowie Vereinigung Baden-Württembergischer Strafverteidiger e.V. (D) (Hrsg.), Strafverteidigung und Inquisition, S. 43.

[67] Botschaft zum Nachrichtendienstgesetz vom 19. Februar 2014, BBl 2014, 2168.

B. Interaktion zwischen Nachrichtendiensten und Strafverfolgungsbehörden – Informationelle Trennung

1. Fehlende Sensibilität für die Notwendigkeit einer informationellen Trennung

Trotz trennender Elemente übersah der Bundesrat schon in einer Vorgängervorlage zum neuen NDG, dass der Nachrichtendienst nicht der Strafverfolgung dienen soll, sondern primär staatsschutzrelevante Bedrohungen erkennen und verhindern soll. Der Bundesrat hielt in der betreffenden Botschaft nämlich fest:

„Sie [die nachrichtendienstliche Beschaffung] kann aber, da sie nur Zugang zum öffentlichen Raum hat, die vermuteten Aktivitäten kaum aufklären und zu einem strafrechtlich relevanten Verdacht verdichten."[68] Genauso undifferenziert ist das Bundesamt für Polizei fedpol, das unter dem Stichwort „Terrorismus" verschiedene Radikalisierungsphasen aufzeigt, in denen die Nachrichtendienst und Strafverfolgungsbehörden chronologisch nacheinander tätig werden. In einer ersten Phase sollen Lehrpersonen, Sozial- und Migrationsbehörden, öffentliche und zivilgesellschaftliche Organisationen wie Opferhilfe- und Beratungsstellen oder Jugendarbeiter erkennen, wenn eine Person anfällig für „ideologische Abwege" ist. Ob diese dem Nachrichtendienst den Verdacht auf „ideologische Abwege" melden sollen, ist nicht ersichtlich und würde auch ungute Erinnerungen etwa an die Staatssicherheitsbehörde in der ehemaligen DDR[69] wecken. Jedenfalls wird der Nachrichtendienst in der zweiten Phase auf eine Person auf ideologischen Abwegen aufmerksam und beobachtet ihre Aktivitäten, um in einer dritten Phase Hinweise an das Bundesamt für Polizei weiterzugeben, dass von der beobachteten Person eine Straftat vorbereitet oder begangen werden könnte oder schon begangen wurde. Das Bundesamt leitet dann erste polizeiliche Ermittlungen in die Wege, um in einer vierten Phase ausreichend belastendes Material zusammenzutragen, damit die Bundesanwaltschaft ein Strafverfahren gegen die Person eröffnen kann. Die nächsten Phasen bestehen in der Verurteilung der Person, dem Strafvollzug und schliesslich der Integration in die Gesellschaft. Bei dieser letzten Phase wird wiederum (unter anderem) der Nachrichtendienst aktiv, um zu beobachten, ob die Person immer noch gefährlich ist.[70] Damit wäre wieder die Phase zwei erreicht auf die wieder Phase drei folgt und so weiter.

Von einer informationellen Trennung von Nachrichtendienst und Strafverfolgungsbehörden kann mithin in der Schweiz nicht ernsthaft gesprochen werden.

---

[68] Botschaft zur Änderung des Bundesgesetzes über Massnahmen zur Wahrung der inneren Sicherheit (Besondere Mittel der Informationsbeschaffung) vom 15. Juni 2007, 5058.

[69] Siehe dazu etwa https://www.bpb.de/geschichte/deutsche-geschichte/stasi/ [Stand 1.7.2021].

[70] Siehe https://www.fedpol.admin.ch/fedpol/de/home/terrorismus/terrorismus-aktuelle-lage/Phasen.html [Stand 1.7.2021].

Zwar findet nicht ein durchgehend ungehinderter Informationsaustausch zwischen Nachrichtendienst und Strafverfolgungsbehörden statt. Aber es bestehen Übermittlungspflichten.

2. Meldungen der Strafverfolgungsbehörden an den Nachrichtendienst

So sind etwa Strafverfolgungsbehörden verpflichtet, dem NDB unaufgefordert zu melden, wenn sie eine konkrete[71] und schwere Bedrohung der inneren Sicherheit feststellen (Art. 20 Abs. 3 NDG).[72] Welche Vorgänge und Feststellungen dem NDB unaufgefordert zu melden sind, legt der Bundesrat in einer nicht öffentlichen Liste fest (Art. 20 Abs. 4 NDG). Das fedpol und der NDB geben sich gestützt auf Art. 5 Abs. 2 NDV gegenseitig Informationen weiter, die sie zur Erfüllung ihrer gesetzlichen Aufgaben benötigen, insbesondere solche nach der eben erwähnten nicht öffentlichen Liste des Bundesrates nach Artikel 20 Absatz 4 NDG. Das gesetzlich geschützte Berufsgeheimnis bleibt bei solchen Auskünften gewahrt (Art. 21 NDG). Bei Meinungsverschiedenheiten zwischen kantonalen Strafverfolgungsbehörden und dem NDB über die Auskunfts- und Meldepflichten entscheidet laut Art. 22 Abs. 2 NDG das Bundesverwaltungsgericht nach Art. 36*a* des Verwaltungsgerichtsgesetzes[73].

3. Meldungen des Nachrichtendienstes an die Strafverfolgungsbehörden

Umgekehrt gibt auch der Nachrichtendienst Informationen an die Strafverfolgungsbehörden weiter. Der Gesetzgeber hat die Weitergabe von Informationen des Nachrichtendienstes an die Strafverfolgungsbehörden in Art. 59 f. NDG geregelt.[74] Gemäss Art. 60 Abs. 2 NDG gibt der NDB seine Erkenntnisse unaufgefordert oder auf Anfrage weiter. Während in Art. 17 BWIS vor Inkrafttreten des NDG (dessen Regelung neu in Art. 60 NDG überführt, dabei aber noch „weiter ausgebaut und differenziert" wurde[75]) der Zeitpunkt der Weitergabe der Erkenntnisse noch geregelt

---

[71] Eine konkrete Bedrohung liegt gemäss Art. 19 Abs. 2 NDG vor, wenn ein bedeutendes Rechtsgut wie Leib und Leben oder Freiheit von Personen oder Bestand und Funktionieren des Staates betroffen ist und die Bedrohung ausgeht von Terrorismus, Spionage, Verbreitung von Massenvernichtungswaffen, Angriffen auf kritische Infrastrukturen oder gewalttätig-extremistischen Aktivitäten.

[72] Siehe auch *Uhlmann*, Untersuchung, Rn. 55; § 4 Basel-Städtische Verordnung über den Vollzug des Bundesgesetzes zur Wahrung der inneren Sicherheit vom 21.09.2010, SG 123.200.

[73] Bundesgesetz über das Bundesverwaltungsgericht (Verwaltungsgerichtsgesetz), SR 173.32.

[74] *Kühne*, AJP 2019, 353.

[75] Botschaft zum Nachrichtendienstgesetz vom 19. Februar 2014, BBl 2014, 2193.

war,[76] fehlt dies in Art. 60 NDG. Vielmehr bleibt es dem Ermessen des NDB überlassen, wann er seine Erkenntnisse weitergibt.[77] Unklar ist auch, wie lange der NDB laufende Ermittlungen weiterführen darf, wenn die Erkenntnisse des Nachrichtendienstes der Strafverfolgung dienen könnten.[78] Gemäss *Gertsch/Stähli* koordinieren in der Praxis die fallbearbeitenden Personen des Nachrichtendienstes und der Strafverfolgungsbehörden ihre Arbeit informell, wobei der Nachrichtendienst so lange tätig bleibt, bis sich ein strafprozessualer Anfangsverdacht bestätigt.[79] Die Befürchtungen der Lehre, dass durch die neuen Befugnisse des NDB dem Strafverfahren vorangestellte fishing expeditions stattfinden können, werden damit noch verstärkt.[80] Das NDG enthält keine Bestimmungen, die eine Umgehung der Bestimmungen der schweizerischen StPO durch die Strafverfolgungsbehörden explizit verhindern würden.

Daten aus genehmigungspflichtigen Beschaffungsmassnahmen werden an die Strafverfolgungsbehörden weitergeleitet, wenn Strafverfolgungsbehörde vergleichbare strafprozessuale Massnahmen anordnen dürfte (Art. 60 Abs. 3 NDG). Sie dürfen im Strafverfahren als Beweise verwertet werden.[81] Art. 60 Abs. 3 NDG gilt als die brisanteste Bestimmung. In ihr wird ein eigentlicher „Bruch strafprozessualer Grundpfeiler“[82] gesehen. Sie lehnt sich an die strafprozessuale Regelung für Zufallsfunde (Art. 278 StPO) an.[83] Das ist problematisch, da Zufallsfunde anlässlich von Ermittlungen gemacht werden, die ihrerseits gestützt auf einen strafprozessualen Anfangsverdacht gemacht werden. Ansonsten ist der Zufallsfund im Strafverfahren nicht verwertbar.[84] Der Nachrichtendienst beschafft die Daten, die er den Strafverfolgungsbehörden weiterleitet, dagegen ohne Tatverdacht. Die strafprozessualen

---

[76] Erkenntnisse, die der Strafverfolgung oder Bekämpfung des organisierten Verbrechens dienen können, waren den Strafverfolgungsbehörden „ohne Verzug“ weiterzuleiten, wenn eine Überwachung des Post- und Fernmeldeverkehrs nach Strafprozessordnung hätte angeordnet werden können. In Bezug auf andere Straftaten konnte die Weitergabe aufgeschoben werden, solange beispielsweise ein überwiegendes öffentliches Interesse zur Wahrung der inneren oder äusseren Sicherheit dem Strafverfolgungsinteresse vorging.

[77] *Schweizer*, plädoyer 4/15, 15.

[78] *Ackermann/Vogler*, NZZ 19. März 2015, 23; *Isenring/Quiblier*, Sicherheit & Recht 3/2017, 130 f.

[79] *Gertsch/Stähli*, in: Kiener/Bühler/Schindler (Hrsg.), Sicherheits- und Ordnungsrecht des Bundes, Rn. 87.

[80] Anderer Ansicht wohl *Bühler*, in: Forum Strafverteidigung (CH), Vereinigung Österreichischer StrafverteidigerInnen (Ö), Initiative Bayerischer Strafverteidigerinnen und Strafverteidiger e.V. (D) sowie Vereinigung Baden-Württembergischer Strafverteidiger e.V. (D) (Hrsg.), Strafverteidigung und Inquisition, S. 26.

[81] *Isenring/Quiblier*, Sicherheit & Recht 3/2017, 131.

[82] *Isenring/Quiblier*, Sicherheit & Recht 3/2017, 130.

[83] Botschaft zum Nachrichtendienstgesetz vom 19. Februar 2014, BBl 2014, 2193 f.

[84] *Ackermann/Vogler*, NZZ 19. März 2015, 23; *Ackermann/Vogler*, in: Ackermann/Hilf, TOP SECRET Geheimnisschutz und Spionage, S. 177. *Isenring/Quiblier*, Sicherheit & Recht 3/2017, 131.

Grenzen könnten nur gewahrt werden, wenn nachrichtendienstliche Erkenntnisse im Strafverfahren unverwertbar wären[85] bzw. gar nicht erst weitergeleitet werden dürften. Dies entspräche auch den unterschiedlichen Zielsetzungen der Tätigkeit von Nachrichtendienst (präventive Tätigkeit zum Schutz der Schweiz) und Strafverfolgungsbehörden (repressive Tätigkeit: Verfolgung und Beurteilung von Straftaten).[86]

Dass die Schweizer Gerichte der kritischen Lehrmeinung folgen, ist zu hoffen. Die Hoffnung wird jedoch durch die bereits vorhandene Rechtsprechung getrübt. Das Bundesgericht hielt in einem Urteil fest, dass die Frage nach der Verwertbarkeit nicht die Eröffnung eines Strafverfahrens betreffe.[87] Dem Amtsbericht wird dann der Charakter einer Strafanzeige zugeschrieben,[88] die zur Eröffnung eines Verfahrens durch die Strafverfolgungsbehörden führen müsse, wenn sie ausreichend Hinweise auf strafbares Verhalten enthält.[89] Das bedeutet, Ermittlungen müssen (bei Offizialdelikten) eingeleitet werden und Zwangsmassnahmen dürfen ergriffen werden.

Der NDB darf wegen der Regelungen zum nachrichtendienstlichen Quellenschutz Erklärungen zur Herkunft seiner Informationen verweigern. Die Gerichte überprüfen folglich nicht, ob Informationen die als Anfangsverdacht dienen, rechtmässig erhoben wurden. Sie vermuten die rechtmässige Erhebung vielmehr und schützen die Verwertbarkeit nachrichtendienstlicher Erkenntnisse auch bei unbekannter Herkunft der Informationen.[90] Der nachrichtendienstliche Quellenschutz ist auch problematisch, wenn der Amtsbericht etwa auf Aussagen von Zeugen verweist, deren Identität der NDB aufgrund des Quellenschutzes nicht preisgibt. Darin läge ein Verstoss gegen das Recht des Beschuldigten, Fragen an Belastungszeugen zu stellen oder zu stellen lassen (Art. 32 Abs. 2 BV[91]; Art. 6 Abs. 3 lit. d EMRK). Dieser Anspruch ist

---

[85] *Pieth*, in: Forum Strafverteidigung (CH), Vereinigung Österreichischer StrafverteidigerInnen (Ö), Initiative Bayerischer Strafverteidigerinnen und Strafverteidiger e.V. (D) sowie Vereinigung Baden-Württembergischer Strafverteidiger e.V. (D) (Hrsg.), Strafverteidigung und Inquisition, S. 17; *Isenring/Quiblier*, Sicherheit & Recht 3/2017, 131.

[86] *Isenring/Quiblier*, Sicherheit & Recht 3/2017, 131.

[87] Urteil vom 27. Januar 2016, 6B_57/2015, 6B_81/2015.

[88] *Gertsch/Stähli*, in: Kiener/Bühler/Schindler (Hrsg.), Sicherheits- und Ordnungsrecht des Bundes, Rn. 82 mit Verweis auf Bundesstrafgericht vom 2. Mai 2014 und Berichtigung der Strafkammer vom 22. Juli 2014 (Strafkammer), Geschäftsnummer, SK.2013.39, E. 2.3.2.

[89] *Bühler*, in: Forum Strafverteidigung (CH), Vereinigung Österreichischer StrafverteidigerInnen (Ö), Initiative Bayerischer Strafverteidigerinnen und Strafverteidiger e.V. (D) sowie Vereinigung Baden-Württembergischer Strafverteidiger e.V. (D) (Hrsg.), Strafverteidigung und Inquisition, S. 24.

[90] Siehe zu dieser Rechtsprechung *Fabbri/Hunkeler*, in: Forum Strafverteidigung (CH), Vereinigung Österreichischer StrafverteidigerInnen (Ö), Initiative Bayerischer Strafverteidigerinnen und Strafverteidiger e.V. (D) sowie Vereinigung Baden-Württembergischer Strafverteidiger e.V. (D) (Hrsg.), Strafverteidigung und Inquisition, S. 41–43; *Von Hahn*, forumpoenale 3/2016, 146–150.

[91] Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999, SR 101.

absolut (und seine Verletzung hätte die Unverwertbarkeit der Beweise zur Folge), falls es sich um für das Urteil wesentliche Aussagen handelt und dem streitigen Zeugnis ausschlaggebende Bedeutung zukommt.[92] Wie das Gericht prüfen soll, zu welchen Anteilen der nachrichtendienstliche Amtsbericht auf Zeugenaussagen beruht, ist jedoch eine andere Frage.

VI. Fazit

Vor 25 Jahren hielt der Bundesrat anlässlich eines Gesetzesentwurfs zur Beschränkung der Befugnisse des Staatsschutzes fest: „Die künftigen Massnahmen des Bundes zur Wahrung der inneren Sicherheit erfassen bewusst nicht jedes mögliche Risiko. In einer freiheitlich demokratischen Ordnung haben der Staat und seine Behörden ein gewisses Störungsrisiko in Kauf zu nehmen.“[93] Diese Einsicht hielt leider nicht lange an. Mit Inkrafttreten des NDG am 1. September 2017 wurde eine 180 Grad Kehrtwende vorgenommen. Der Bundesrat befand, dass das Instrumentarium nicht mehr ausreiche, „um die präventiven Aufgaben des NDB angesichts der immer aggressiveren Akteure, die die innere oder die äussere Sicherheit der Schweiz bedrohen und angesichts der komplexeren Bedrohungsformen weiterhin wahrzunehmen.“[94] Der NDB erhielt deshalb neue Befugnisse, die teilweise über die Befugnisse der Strafverfolgungsbehörden hinausgehen. Zwar verfolgen Nachrichtendienste, Polizei und Strafverfolgungsbehörden unterschiedliche Ziele, es gibt aber Überschneidungsbereiche, da die Nachrichtendienste auch Kriminalitätsfelder beobachten. Ihre Informationen beschaffen sie dabei ohne einen strafprozessualen Anfangsverdacht. Das ist problematisch, da in der Schweizer Praxis die Sensibilität für die Notwendigkeit eines (auch informellen) Trennungsgebots fehlt und die Erkenntnisse des Nachrichtendienstes an die Strafverfolgungsbehörden weitergeleitet werden. Die Strafverfolgungsbehörden koordinieren die Zusammenarbeit mit dem Nachrichtendienst sogar informell und können so problemlos eine in Strafverfahren verbotene fishing expedition mit Hilfe des Nachrichtendienstes durchführen. Die nachrichtendienstlichen Erkenntnisse werden im Anschluss mittels Amtsbericht an die Strafverfolgungsbehörden weitergegeben. Die Rechtsprechung geht bei einem Amtsbericht des Schweizer Nachrichtendienstes ohne weiteres davon aus, dass die darin enthaltenen Informationen rechtmässig beschafft worden sind. In der Schweiz findet somit durchaus Verbrechensbekämpfung durch Nachrichtendienste statt. Zu begrüssen ist das indes nicht. Vielmehr sollte sich der Nachrichtendienst auf den Schutz der Sicherheit der Schweiz beschränken.

---

92 Siehe etwa BGE 131 I 476, 481; 125 I 127, 135.

93 Botschaft zum Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit und zur Volksinitiative «S.O.S. Schweiz ohne Schnüffelpolizei» vom 7. März 1994, BBl 1994 II 1130.

94 Botschaft zum Nachrichtendienstgesetz vom 19. Februar 2014, BBl 2014, 2107.

Literaturverzeichnis

Ackermann, Jürg-Beat/Vogler, Patrick, Der Nachrichtendienst und die Strafprozessordnung. NZZ vom 19.3.2015, 23 (online abrufbar: https://www.nzz.ch/meinung/debatte/der-nachrichtendienst-und-die-strafprozessordnung-1.18505283 [Stand 1.7.2021]).

Ackermann, Jürg-Beat/Vogler, Patrick, Nachrichtendienst und Strafprozess – zur Verwertbarkeit von Beweisen zwischen Systemen. In: Jürg-Beat Ackermann/Marianne Johanna Hilf, TOP SECRET Geheimnisschutz und Spionage. Zürich 2015, 161–187.

Bucherli, Roman, Die seltsame Hinterlassenschaft des Staatsschutzes. NZZ vom 13.7.2009 (online abrufbar: https://www.nzz.ch/die_seltsame_hinterlassenschaft_des_helvetischen_staatsschutzes-1.3015643 [Stand 1.7.2021]).

Bühler, Jürg, Schnittstellen zwischen Nachrichtendienst (Geheimdiensten) und Staatsanwaltschaft. In: Forum Strafverteidigung (CH), Vereinigung Österreichischer StrafverteidigerInnen (Ö), Initiative Bayerischer Strafverteidigerinnen und Strafverteidiger e.V. (D) sowie Vereinigung Baden-Württembergischer Strafverteidiger e.V. (D) (Hrsg.), Strafverteidigung und Inquisition, 6. Dreiländerforum Strafverteidigung, Basel, 10./11. Juni 2016 (Schriftenreihe der Vereinigung Österreichischer StrafverteidigerInnen – Band 30), Wien/Graz 2017, 21–26.

Clavadetscher, Richard, ÜBERWACHUNG: Die Fichenaffäre wirkt bis heute nach. Luzerner Zeitung vom 27.8.2016 (online abrufbar: https://www.luzernerzeitung.ch/schweiz/ueberwachung-die-fichenaffaere-wirkt-bis-heute-nach-ld.83523 [Stand 1.7.2021]).

Fabbri, Alberto/Hunkeler, Thomas, Herausforderungen für Kriminalpolizei und Staatsanwaltschaft im Zusammenhang mit dem Nachrichtendienst. In: Forum Strafverteidigung (CH), Vereinigung Österreichischer StrafverteidigerInnen (Ö), Initiative Bayerischer Strafverteidigerinnen und Strafverteidiger e.V. (D) sowie Vereinigung Baden-Württembergischer Strafverteidiger e.V. (D) (Hrsg.), Strafverteidigung und Inquisition, 6. Dreiländerforum Strafverteidigung, Basel, 10./11. Juni 2016 (Schriftenreihe der Vereinigung Österreichischer StrafverteidigerInnen – Band 30), Wien/Graz 2017, 27–54.

Gerny, Daniel, Das Nachrichtendienstgesetz auf einen Blick. NZZ vom 18.8.2016 (online abrufbar: https://www.nzz.ch/schweiz/abstimmung-vom-25-september-das-nachrichtendienstgesetz-auf-einen-blick-ld.111204 [Stand 1.7.2021]).

Gertsch, Gabriel/Stähli, Armin, Nachrichtendienstlicher Staatsschutz. In: Regina Kiener/René Bühler/Benjamin Schindler (Hrsg.), Sicherheits- und Ordnungsrecht des Bundes, Teil 2, Besonderer Teil. Basel 2018, S. 431–439.

Isenring, Bernhard/Quiblier, Laura, Der Preis der Sicherheit. Sicherheit & Recht, 3/2017, 127–140.

Kreis, Georg, Staatsschutz in der Schweiz. Die Entwicklung von 1935-1990, Bern 1993.

Kühne, Stefan/Rütsche, Serdar Günal, GovWare-Einsatz – nur zur Fernmeldeüberwachung oder auch zur technischen Überwachung? AJP 2019, 350–357.

Meier, Dominik, Ruf nach mehr Ressourcen, SRF 19. Oktober 2018, abrufbar unter: https://www.srf.ch/news/schweiz/ruf-nach-mehr-ressourcen-der-hungrige-nachrichtendienstchef [Stand 21.7.2021].

Niggli, Marcel Alexander/Heer, Marianne/Wiprächtiger, Hans (Hrsg.), Basler Kommentar, Schweizerische Strafprozessordnung, Jugendstrafprozessordnung. 2. Aufl. Basel 2014 (zit. BSK StPO-*Bearbeiter*).

Pieth, Mark, Strafverfolgung in der Dunkelkammer: Eine rechtspolitische Bestandesaufnahme. In: Forum Strafverteidigung (CH), Vereinigung Österreichischer StrafverteidigerInnen (Ö), Initiative Bayerischer Strafverteidigerinnen und Strafverteidiger e.V. (D) sowie Vereinigung Baden-Württembergischer Strafverteidiger e.V. (D) (Hrsg.), Strafverteidigung und Inquisition, 6. Dreiländerforum Strafverteidigung, Basel, 10./11. Juni 2016 (Schriftenreihe der Vereinigung Österreichischer StrafverteidigerInnen – Band 30), Wien/Graz 2017, 9–20.

Rauber, Philipp, Rechtliche Grundlagen der Erfüllung sicherheitspolizeilicher Aufgaben durch Private. Basel u.a. 2006.

Reinhard, Hans, Allgemeines Polizeirecht. Aufgaben, Grundsätze und Handlungen. Bern u.a. 1993.

Roos, Eveline /Jeker, Konrad, Der «Grosse Lauschangriff». forumpoenale 2017, 412–417.

Schweizer, Rainer J., Unkontrollierbare Überwachung ruiniert den Rechtsstaat und die freiheitliche Demokratie, plädoyer 4/15, 14–17.

Steiger, Martin, Neues Nachrichtendienstgesetz in der Schweiz: Sicherheitsesotherik statt Menschenrechte, netzpolitik.org, 12.01.2016 (https://netzpolitik.org/2016/neues-nachrichtendienstgesetz-in-der-schweiz-sicherheitsesoterik-statt-menschenrechte/ [Stand 1.7.2021]).

Steiger, Martin, Sicherheitsesoterik statt Menschenrechte. Zeitschrift für Datenrecht und Informationssicherheit (digma) 2015, 134–137.

Uhlmann, Felix, Untersuchung in Sachen Kantonspolizei Basel-Stadt betreffend Massnahmen gegen einen Mitarbeiter der Kantonspolizei (Hinweis des NDB) im Auftrag des Justiz- und Sicherheitsdepartements Basel-Stadt, 14. Juni 2017 (abrufbar unter: https://www.polizei.bs.ch/nm/2017-untersuchung-uhlmann-kantonspolizei-hat-gehandelt-aber-hindernisse-zu-wenig-hinterfragt-jsd.html [Stand 1.7.2021]).

von Hahn, Patrick, Nr. 21 Bundesgericht, Strafrechtliche Abteilung, Urteil vom 27. Januar 2016 i.S. A.X. und B.X. gegen Schweizerische Bundesanwaltschaft – 6B_57/2015, 6B_81/2015, Urteilsbesprechung. forumpoenale 2016, 146–150.

Wohlers, Wolfgang, Informationsverbund von Nachrichtendienst und Strafbehörden. Rütteln an den Eckwerten des modernen Strafverfahrens. NZZ vom 18.7.2007, 15 (online abrufbar: https://www.nzz.ch/informationsverbund_von_nachrichtendienst_und_strafbehoerden-1.529363 [Stand 1.7.2021]).

Wohlers, Wolfgang, Rezension: Forum Strafverteidigung (CH), Vereinigung Österreichischer StrafverteidigerInnen (Ö), Initiative Bayerischer Strafverteidigerinnen und Strafverteidiger e.V. (D) sowie Vereinigung Baden-Württembergischer Strafverteidiger e.V. (D) (Hrsg.), Strafverteidigung und Inquisition, 6. Dreiländerforum Strafverteidigung, Basel, 10./11. Juni 2016 (Schriftenreihe der Vereinigung Österreichischer StrafverteidigerInnen – Band 30), Wien/Graz 2017. ZStrR 2017, 469.

Zurkinden, Nadine, Joint Investigation Teams. Chancen und Grenzen von gemeinsamen Ermittlungsgruppen in der Schweiz, Europa und den USA, Berlin 2013.

Abkürzungsverzeichnis

AJP	Aktuelle Juristische Praxis
BS	Basel-Stadt
BSK	Basler Kommentar
BV	Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999, SR 101
BWIS	Bundesgesetz vom 21. März 1997 über Massnahmen zur Wahrung der inneren Sicherheit, SR 120
EDA	Eidgenössisches Departement für auswärtige Angelegenheiten
EJPD	Eidgenössisches Justiz- und Polizeidepartement
fedpol	Bundesamt für Polizei
NDB	Nachrichtendienst des Bundes
NDG	Bundesgesetz vom 25. September 2015 über den Nachrichtendienst (Nachrichtendienstgesetz), SR 121
NDV	Verordnung vom 16. August 2017 über den Nachrichtendienst (Nachrichtendienstverordnung), SR 121.1
NZZ	Neue Zürcher Zeitung
SG	Systematische Gesetzessammlung Kanton Basel-Stadt
SR	Systematische Rechtssammlung
SRF	Schweizer Radio und Fernsehen
StGB	Schweizerisches Strafgesetzbuch vom 21. Dezember 1937, SR 311.0
StPO	Schweizerische Strafprozessordnung vom 5. Oktober 2007 (Strafprozessordnung), SR 312.0
VBS	Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport
ZEO	Zentrum für elektronische Operationen der Schweizer Armee

Combating Crime through Intelligence Services

The Spanish case

Susana Sánchez Ferro

1. Introduction

In the Cold War adversaries used very hierarchical, familiar and predictable military command and control methods.[1] When the Cold War came to an end, the vacuum caused by the sudden demise of the Soviet Union created fresh sources of

[1] The 9/11 Commission Report, p. 87.

instability and new challenges, such as international terrorism; threats were less visible and surpassed the boundaries of traditional nation states. As technology developed and globalization grew, dangers were more immediate and required an agile and quick response.[2] The organization of the intelligence community was no longer suitable to confront these dangers and had to evolve.

Amongst the recommendations of The 9/11 Commission Report in the USA, after the terrorist attacks on its soil, the Commission asked for the need to unify strategic intelligence and operational planning against Islamic terrorists "across the foreign-domestic divide with a National Counterterrorism Center", to create a new National Intelligence Director to unify the intelligence community, and to unify the many participants in the counterterrorism effort and their knowledge in a network-based information-sharing system that transcended traditional governmental boundaries.[3] The Commission also recommended that the FBI shift its posture from a more criminal justice mission to a national security mission, moving toward a more "preventive counterterrorism posture."[4] The U.S. example serves to illustrate the evolution experienced by the security and intelligence services regarding their organization and main tasks in the past few years.

In Spain, the need for intelligence to be more operative in order to confront the terrorist threat has also been underlined. Antonio Díaz, one of our experts in intelligence services, advocates for a closer relationship between police forces and the intelligence service, and thinks they should take part in crisis mechanisms as well, without disregarding the need for strategic intelligence elaborated by the intelligence service. This qualitative change in our model of intelligence should lead to the creation of new structures and capacities, the increase of personnel and funds for the intelligence service and the adoption of new instruments and legal rules in order to adapt to these changes.[5]

2. The Spanish Security Architecture

2.1 The Intelligence Service

a) Shaping an intelligence service in a world of nation states

Spain became a democracy in the late 1970s. In 1975 General Franco died, but the democratic general elections took place in 1977. The world was still a world of nation states; the Cold War had not come to an end. In this scenario, Prime Minister

---

[2] The 9/11 Commission Report, pp. 87, 89, 399, 340.

[3] The 9/11 Commission Report, pp. 399–340.

[4] The 9/11 Commission Report, pp. 423, 425.

[5] *Díaz Fernández, Antonio M.*: ARI Nº 52/2006, pp. 1–2.

Suárez decided to create a new intelligence service – the Centro Superior de Información de la Defensa or CESID [Superior Center of Information for Defense] – by Royal Decree.[6] The Spanish Constitution of 1978 was not yet in force.

The CESID replaced the SECED [Servicio Central de Documentación – Central Documentation Service], the intelligence service of Franco's Prime Minister Carrero Blanco, and the military intelligence service, which was then under the command of the Joint Chiefs of Staff.[7] The Government decided to put the CESID under the Department of Defense. Initially, almost all of its personnel appertained exclusively to the armed forces.[8] In fact, the director had to be a General with the category of Director General, according to the law.[9]

General Gutiérrez Mellado, Minister of Defense in the Suárez era (transition to democracy), wanted to divert intelligence from the military and leave only the intelligence directly related to military issues to the military. He transferred incardinated the intelligence service to the Department of Defense and created a generalist service. He wanted the new service to inform the Executive about possible subversive movements inside the military.[10] A Royal Decree defined the Center's mission. The Center would be in charge of obtaining, evaluating, interpreting and providing the head of the Defense Department with as much information as was necessary or of interest to the national defense, attending primarily to the needs of the board of Chiefs of Staff.[11]

In 1978 the Spanish Constitution was passed. During the first four years of existence, the CESID was not subject to clear guidelines (the Center had four different directors). There was a need for a change in the intelligence service, even more

---

[6] S. 2.5 Royal Decree 1558/1977, of 4th July, restructuring some Organs of the Central Administration (Artículo 2.5 del Real Decreto 1558/1977, de 4 de julio, por el que se reestructuran determinados Órganos de la Administración Central del Estado). See https://www.cni.es/es/queescni/historia/elcesid/ (web page of the Spanish intelligence service). Even if it might seem unbelievable, the Spanish Parliament did not pass a law regulating the Spanish intelligence services until 2002.

[7] The SECED was created in March 1972, ascribed to the Minister Undersecretary of the Presidency and its members were all military. Its main task was to obtain and analyse information and give intelligence to the Minister, but it also carried out some operations against ETA, the terrorist group/Basque Country separatist movement. In the summer of 1975 *Operation Wolf* (Operación Lobo) decapitated the terrorist group. *Díaz Fernández, Antonio M.*, Un actor político, pp. 205, 207 and 208.

[8] https://www.cni.es/es/queescni/historia/elcesid/

[9] S. 21 (2) Royal Decree 2723/1977, of 2nd November, which reorganized the Minister of Defense [Real Decreto 2723/1977, de 2 de noviembre, por el que se estructura orgánica y funcionalmente el Ministerio de Defensa].

[10] *Díaz Fernández, Antonio M.*: Un actor político, p. 213. *Ruíz Miguel, Carlos*: El CESID, p. 126. On the discussion about whether the CESID had the power to oversee possible subversive movements in the Military, see *Díaz Fernández, Antonio M.*: Un actor político, pp. 214–215.

[11] S. 21 (1) Royal Decree 2723/1977.

obvious after the coup d'état of 1981, as some of the participants in the coup were members of the CESID and the old SECED.[12] From 1982 onwards the CESID was modernized; its structures and objectives were adapted to the internal and external needs of the country, and the Government proceeded to institutionalize it, regulating its structure and missions in much more detail, though no statute regulated its mission yet (the Constitution did not refer to the intelligence service either).[13]

In 1982, the CESID still depended organically on the Ministry of Defense, but functionally, the Center was in charge of providing intelligence not only to the Defense Department, but also to the Prime Minister in order for him to guide Defense Policy.[14] On the other hand, despite the exclusive reference to the field of defense, the executive order assigned to the CESID tasks related to the maintenance of the constitutional order, including for the first time the task of providing intelligence to the Prime Minister in order to fight those who attacked this institutional order, destabilizing the country (the Executive was thinking of ETA and other internal terrorist groups which were very active in those days, threatening and damaging the constitutional order).[15] The Spanish intelligence service had, therefore, a very broad experience in the fight against national terrorism. After the fall of the Berlin Wall it had to face a new kind of terrorism – international terrorism.

---

[12] *Díaz Fernández, Antonio M.*: Teoría de las organizaciones, p. 23. A discussion about the role of the CESID in the coup d'état in *Díez Fernández, Antonio M.*: Un actor politico, pp. 214–216.

[13] *Díaz Fernández, Antonio M.*: Un actor político, p. 217. *Ruiz Miguel, Carlos*: El CESID, p. 125. The CESID was regulated by executive royal decrees and orders until 2002. See Royal Decree 726/1981 [Real Decreto 726/1981, de 27 de marzo, por el que se modifica el Real Decreto 2723/1977, de 2 de noviembre, que estructura orgánica y funcionalmente el Ministerio de Defensa]; Ministerial Order 135/1982 [Orden 135/1982, de 30 de septiembre, por la que se regula la estructura y relaciones que ha de mantener el Centro Superior de Información de la Defensa]; Royal Decree 135/1984 [Real Decreto 135/1984, de 25 de enero, por el que se reestructura el Ministerio de Defensa]; Royal Decree 2632/1985 [Real Decreto 2632/1985, de 27 de diciembre, por el que se regula la estructura interna y las relaciones del Centro Superior de Información de la Defensa]; Royal Decree 1169/1995 [Real Decreto 1169/1995, de 7 de julio, por el que se modifica la estructura orgánica del Centro Superior de Información de la Defensa]; Royal Decree [Real Decreto 1324/1995, de 28 de julio, por el que se establece el Estatuto del Personal del Centro Superior de Información de la Defensa] and Royal Decree 266/1996 [Real Decreto 266/1996, de 16 de febrero, por el que se modifica la estructura orgánica básica del Centro Superior de Información de la Defensa].

[14] Sections 1 & 2 of the Ministerial Order 135/1982.

[15] In 1980, for example, ETA killed 92 people [Source: Internal Affairs Minister (www.mir.es): Subdirección General de Atención al Ciudadano y a las Víctimas del Terrorismo November 2009]. This was the year with more victims of ETA terrorism. The CNI webpage – the CNI is the new intelligence service – states that the Intelligence Center had as one of its goals the fight against terrorism since the time of Minister Rodríguez Sahagún, who served as Defense Secretary from 6th April 1979 to 26th February 1981 [https://www.cni.es/es/queescni/historia/elcesid/]. The CESID was also given competences related to external security for the first time. *Ruiz Miguel*, *Carlos*: El CESID, p. 126.

According to section 3 of the Ministerial Order 135/1982, the Center would have the following missions:

– To *obtain, evaluate and disseminate* the necessary *information* to prevent any *danger, threat or external aggression* against the independence or territorial integrity of Spain and to ensure its national interests. Such information will cover political, economic, technological and military issues.
– To *counteract espionage and the activities of foreign intelligence services* that commit an outrage against national security or the national interest, through their prevention, detection and neutralization inside and outside the national territory.
– To guarantee *the security of information, technology, procedures, objectives and facilities of interest for the defense* (our own and those of allied countries), excluding those under the direct competency of the armed forces.
– To obtain, evaluate and disseminate information related to internal processes that, through anti-constitutional procedures, would go against the unity of the homeland and the stability of its fundamental institutions.

According to those missions, Section 2 (1) of the Royal Decree 2632/1985 established that the CESID would be divided into the following divisions: External Intelligence Division;[16] Division of Counterintelligence;[17] Internal Intelligence Division;[18] Division of Economy and Technology;[19] General Sub Direction of Administration and Services and General Sub Direction of Personnel.[20] There would be an Operations Office (Jefatura de Apoyo Operativo) in order to, amongst other tasks, carry out those activities that require special means, procedures or techniques

---

[16] The External Division would obtain, evaluate and disseminate the information to prevent any danger, threat or foreign aggression against the independence or territorial integrity of Spain, ensuring its national interests; such information would cover political, economic and military fields (s. 4 Royal Decree 2632/1985).

[17] The Division of Counterintelligence would counter espionage and the activities of the foreign intelligence services that were against security or the national interest, through its prevention, detection and neutralization inside and outside the national territory (s. 5 Royal Decree 2632/1985).

[18] The Division of Internal Intelligence would obtain, evaluate and disseminate the information regarding internal processes that, by anti-constitutional procedures, attacked the unit of Spain and the stability of its institutions (s. 6 Royal Decree 2632/1985).

[19] The division of Economy and Technology would have to obtain, evaluate and disseminate the necessary information to prevent any danger, threat or foreign aggression against the Spanish industry and trade of weapons and war material. It shall protect the national interests in the fields of economy and technology of specific interest for the defense, and guarantee the security of the information, technology, procedures, objectives and facilities of interest for the Spanish and allied defense (s. 7 Royal Decree 2632/1985).

[20] Royal Decree 1/1987, of 1st January [Real Decreto, de 1 de enero, por el que se determina la Estructura Orgánica Básica del Ministerio de Defensa] gave the CESID the task of coordinating the actions of the different organs that use means or procedures of encryption, to guarantee the cryptographic security, and to promote the acquisition of material and form the specialist personnel.

that were "previously and duly authorized". This Unit was in the spotlight when on June 12th, 1995 the press published that the CESID had been intercepting the conversations of politicians, the press, businessmen and even the King and some of his friends during the previous ten years.[21] Royal Decree 266/1996 also introduced a reference to this support unit for the intelligence units. This unit would be in charge of operational and technical support when the mission of the intelligence units required special means, procedures or techniques.[22]

b) New challenges for a renewed Intelligence Service: Facing the 21st Century

After the terrorist attacks of 9/11, the Spanish Parliament passed an act regulating the new national intelligence service, the CNI [National Intelligence Center]. The CNI replaced the CESID [Act 11/2002, of 6th May, regulating the National Intelligence Center, from now on the CNI Act].[23] Parliament thought there was a need to adapt the structures and operation of the old CESID to the new requirements of national security; to provide the intelligence service with the necessary tools to fulfill the objectives assigned to them; and to create a unitary and systematic regulation with the appropriate legal rank in light of the Constitution.

The new law integrated the CNI in the Department of Defense – Ministerio de Defensa (s. 7 (1) CNI Act), but allowed the Prime Minister to change this adscription by Royal Decree (Additional Clause n.3). The Prime Minister made use of this possibility and in 2011 the CNI organically came under the Department of Presidency [Ministerio de Presidencia].[24] In 2018, after the socialist group won a vote of no confidence, the CNI was included again in the Department of Defense [Ministerio de Defensa].[25] The preamble of Royal Decree 436/2002, which establishes the structure of the CNI, insists on the importance of establishing a flexible structure for the intelligence service in order to facilitate a better fulfillment of the Center goals.[26]

---

[21] See https://www.elmundo.es/especiales/2007/10/comunicacion/18elmundo/cesid.html. The courts considered the interceptions of those communications as illegal [Sentencia de la Audiencia Provincial de Madrid de 4 de abril de 2005 & Sentencia del Tribunal Supremo 921/2006, 26 de septiembre de 2006]. In March of 1998, the press also unveiled that the CESID had been spying on the seat of the political party Herri Batasuna, the political arm of ETA.

[22] S. 2 (2) of Royal Decree 266/1996, modifying the structure of the CESID [Real Decreto 266/1996, de 16 de febrero, por el que se modifica la estructura orgánica básica del Centro Superior de Información de la Defensa].

[23] Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia.

[24] 2nd Additional Clause of Royal Decree 1823/2011 [Real Decreto 1823/2011, de 21 de diciembre, por el que se reestructuran los departamentos ministeriales].

[25] 2nd Additional Clause, Royal Decree 355/2018 [Real Decreto 355/2018, de 6 de junio, por el que se reestructuran los departamentos ministeriales].

[26] Royal Decree 436/2002, of 10th May, establishing the organic structured of the CNI. Since the mid-1990s, the intelligence agencies in different countries are structured mainly

The Government, through Royal Decrees, changed its structure, giving more weight to the operational department, probably to satisfy the growing demand for operational intelligence after 9/11.

The CNI is led by an Undersecretary [Secretario de Estado] designated by the Secretary of State for Defense – Ministro de Defensa (s. 9 (1) CNI Act), and in 2001 the CESID had its first civil director.[27] Although organically the CNI is part of the Department of Defense, functionally it is independent so as to gain flexibility; it has an autonomous regime regarding personnel, budget and recruitment (s. 7 (2) CNI Act).[28] But who are the spies? In the beginning CESID personnel were almost exclusively military personnel that came from the SECED and the military; later on the number of civilians in its ranks increased: in the year 2012 only 28.55% of its personnel were military personnel, 59.88% of its workforce came from the civilian field, and 11.57% from the police forces; in 2015, only 27% of CNI's members came from the armed forces and 10% from the police forces, in particular from the Guardia Civil, which were in charge of operational functions, but they still occupied the most important positions of the service, for example, in the area of terrorism or in support of the military operations of Spain in Iraq, Afghanistan, Libya, Mali or the Indian Ocean.[29]

Until 1995, when the Government passed Royal Decree 1324/1995 on 28th July, there was no special legal regime applicable to the CESID personnel. The CESID personnel came from the armed forces, the civil service, the security services, the academy and the private sector.[30] All were subject to different employment conditions and specific legal regimes applicable to their own sector. In order to solve this disparity in legal regimes, Law 17/1989 of 19th July mandated that all the CESID personnel should be subject to the same legal status regarding their employment

---

in three major branches: the informative/intelligence, operations and the administrative branch [*Díaz Fernández, Antonio M.*: La adaptación, p. 5].

[27] https://www.cni.es/es/queescni/historia/elcesid/

[28] The CNI is an autonomous public organ according to the First Additional Provision of the CNI Act. Article 98 of the 40/2015 Act of 1st October, regulating the legal system of the public sector defines those autonomous organs inside the administration as organs of public law, with their own juridical personality, Treasury and own patrimony and autonomy in their management; and considers them as General Administration's instrumental organizations.

[29] On the 2012 numbers, see *Martínez Sánchez, Juan Antonio*: El reclutamiento, p. 203. On the 2015 numbers, see https://elpais.com/elpais/2015/12/02/eps/1449074403_164457.html. According to this article in *El País*, in 2015 there were around 3500 agents in the CNI with a budget of 240 million euros. Outside Spain, the CNI had contacts in all the embassies, with agents with diplomatic status and also with clandestine collectors. In 2015 there were some 200 professionals, and an indeterminate number of contractors, which is called the Intelligence Reserve.

[30] At the end of 1982, Colonel Manglano opened the door to the entry of civilians as intelligence analysts and technology experts. A year later, in May 1983, the door was also opened to women. https://elpais.com/elpais/2015/12/02/eps/1449074403_164457.html.

conditions, rights and duties.[31] By Royal Decree (Royal Decree 1324/1995) the Government approved the first unified legal regime for the spies, afterwards superseded by Royal Decree 240/2013 of 5th April.[32] Only those who become public employees could exercise the functions attributed by law to the CNI. Those who were already public servants, like policemen, the Guardia Civil or the military, can serve temporarily or permanently in the CNI, transferring to a special administrative status compared to their original position (ss. 2 & 14 Royal Decree 240/2013).[33] If they return to their original position in the police force or the military they have a legal duty of confidentiality regarding the activities of the CNI, its organization and internal structure, means and methods, facilities, data bases and data centers, sources and any other information or data that can reveal those elements, subject to the official secrets legislation (ss. 75 & 109 Royal Decree 240/2013).

Royal Decree 2632/1985 established a structure of the old CESID to fit the functions of the intelligence service: external intelligence, counterintelligence, internal intelligence and economy and technology intelligence. The new 2002 CNI Act widened the scope of the intelligence service tasks; the CNI Act allows the CNI to act inside or outside Spain in order to obtain, evaluate and interpret information and disseminate the necessary intelligence to *protect and promote the political, economic, industrial, commercial and strategic interests of Spain* (s. 4 (a) CNI Act). The CNI has an internal and external remit; it must *prevent, detect and enable the neutralization* of those foreign services, groups or person's activities that put at risk, threaten or attack the *constitutional order, the rights and freedoms of Spanish citizens, the sovereignty, integrity and security of the state, the stability of its institutions, the national economic interests and the welfare of the population* (s. 4 (b) CNI Act). At the end of 2001, the CESID created, at the behest of the director Dezcallar, a unit in charge of non-national terrorism composed of about twenty agents. After the terrorist attacks in Madrid in March 2004, this unit increased its number of agents to forty.[34]

The CNI is also in charge of the *cybersecurity* of the administration (s. 4 (e) CNI Act) and the protection of classified information, as well as the protection of the personnel and material means and facilities of the Center (s. 4 (f) CNI Act).

---

[31] 8th final clause of Law 17/1989, regulating the legal regime of the military and professional personnel.

[32] Real Decreto 240/2013, de 5 de abril, por el que se aprueba el Estatuto del personal del Centro Nacional de Inteligencia.

[33] The maximum period to work in a temporary capacity in the CNI as a public servant is six years. After serving five years in the CNI personnel are offered to remain as permanent workers in the CNI or are dismissed for not being adequate for the job (s. 13 Royal Decree 240/2013).

[34] *Díaz Fernández, Antonio M.*: La adaptación, p. 3.

Additionally, for the first time the law included a provision giving the Government the exclusive power to establish the aims to be pursued by the intelligence service in the Intelligence Directive (s. 3 CNI Act). This Intelligence Directive is secret (s. 3 CNI Act). The law assigns the Center the task of obtaining, evaluating and interpreting the traffic of strategic signals, for the fulfillment of intelligence objectives (s. 4 d) CNI Act).

Despite the breadth of the tasks assigned, the CNI missions are still involved with the protection of the sovereignty and integrity of the State and constitutional order[35] (which was the remit of the old External Division), the protection of the rights and freedoms of Spanish citizens and the stability of the institutions (Internal Division), the protection of economic interests and welfare of the population (Economic Division), and the neutralization of foreign espionage (Counterespionage Division).[36]

In 2002 the CNI was structured into two departments or directions, one in charge of intelligence and counterintelligence and another one dedicated to the administration of the Center (the so-called direction of resources), introducing for the first time a clear separation between the Intelligence Department and the administration of the Center.[37] In 2006 the structure changed to three departments: a technical directorate of intelligence, under the oversight of the CNI Director (with the rank of Undersecretary), a directorate to support intelligence (like the old operations office), also under the oversight of the CNI Director, and a directorate of resources, under the oversight of the secretary general of the CNI (who is directly under the command of the CNI director), all of which are now under the oversight of the secretary general.[38] Therefore, the operations branch increased its importance in the structure of the CNI. According to *El País* (the Spanish newspaper), in 2015 the CNI was structured into 18 divisions, and then in departments and areas. In those areas the division is in transversal, thematic and geographical groups.[39]

---

[35] In the project of the Constitution the defense of the Constitutional order was assigned to the police, but in the discussions of the project members of Parliament agreed that the defense of constitutional order was the mission of the army [see *Barcelona Llop, Javier*: Policía y Constitutión, pp. 226–227].

[36] The division of economy and technology was included inside the division for counterintelligence; see *Díaz Fernández, Antonio M.*: Teoría de las organizaciones, p. 35.

[37] Ss. 1(c) and 4 Royal Decree 436/2002 of 10th May regulating the structure of the CNI. *Díaz Fernández, Antonio M.*: Teoría de las organizaciones, p. 35.

[38] The office of operational support was converted in a direction under the direct dependency of the CNI Director in 2006, when the Government passed Royal Decree 612/2006 of 19th May, which modified Royal Decree 436/2002 of 10th May [Real Decreto 436/2002, de 10 de mayo, por el que se establece la estructura orgánica del Centro Nacional de Inteligencia]. The First Final Clause of Royal Decree 240/2013 of 5th April regulating the personnel status of the CNI mandated that the three different directions would depend on the Secretary General.

[39] https://elpais.com/elpais/2015/12/02/eps/1449074403_164457.html

2.2 The Police Forces and Their Missions

Article 104 of the Spanish Constitution (SC) assigns the police forces, a branch of the Government, the mission to protect the free exercise of the rights and freedoms of citizens and to guarantee citizens' security. Those police forces with a national remit consist of the Cuerpo Nacional de Policía (or Policía Nacional), an armed institute of a civil nature, and the Guardia Civil, an armed institute of a military nature, both part of the Home Department, except when the Guardia Civil carries out military missions under the orders of the Defense Department.[40] The police forces are law enforcement agencies that must protect the people, goods and civic order against any danger through preventive measures and, if necessary, through the use of force or coercion.[41]

Although article 104 SC refers only to the police forces under Government command, article 149.1.29 SC allows for the existence of police forces in the autonomous communities if they assume this power in their *Estatutos de Autonomía*, the superior norm of the Autonomies under the Constitution [there are police forces in Catalonia – Mossos d'Escuadra – Navarra – Policía Foral de Navarra – and the Basque Country – Ertzainza].[42]

Article 126 SC, on the other hand, assigns the police forces (Policía and Guardia Civil), as well as the police forces of the autonomous communities, and the local police, the functions of investigating crime and discovering and securing the offender. To fulfill this function, the different police forces are functionally under the command of the judges, the courts and the public prosecutor (judicial police), although organicasationally they continue to be within the Home Department.[43] Criminal conduct constitutes the starting point for the intervention of the police forces under the guidance of public prosecutors and judges.[44]

Therefore, the police forces in Spain act in two different spheres: Defense against risks or dangers to citizens' security (*Gefahrabwehr*) under the authority of the Security Undersecretary [Secretario de Estado de Seguridad], and prosecution of criminal wrongdoing (*Strafverfolgung*) under the judges or public prosecutor's

---

[40] S. 9 Organic Law 2/1986, of 13th March, regulating the Security Forces [Ley Orgánica 2/1986, de 13 marzo, de Fuerzas y Cuerpos de Seguridad].

[41] *Parejo Alfonso*, *Luciano*: Seguridad Pública, p. 65.

[42] Articles 1 and 2 of the Organic Law 2/1986, of 13th March, regulating the Security Forces refers to the Policía and Guardia Civil, autonomous communities' Police and Local Police as Security Forces.

[43] Article 31.1 Organic Law 2/1986: in the performance of their duties, officials attached to judicial police units depend organisationally on the Ministry of the Interior and functionality of the judges, tribunals or prosecutors who are aware of the subject matter of their investigation.

[44] *Parejo Alfonso, Luciano*: Seguridad Pública, pp. 20–21. When police forces are investigating an act alleged to amount to a crime before the judge intervenes, they will act under the orders of the public prosecutor. *De la Oliva Santos et al.*: Derecho Procesal Penal, p. 107.

[Ministerio Fiscal] command.[45] According to article 11 of the Security Forces Act,[46] police forces shall ensure compliance with the laws and general provisions, protect people and ensure the conservation and custody of property if it is in danger, and maintain and restore, where appropriate, public order and security; they must also prevent the commission of criminal acts and investigate offenses to discover and detain the suspects, secure the instruments of the crime, effects and evidence of the offense, and make them available to the competent judge or court.[47]

Interestingly enough, the police forces are in charge of obtaining, receiving and analyzing all data of interest to civic order and security, and of planning and carrying out methods and techniques in order to prevent crime (s. 11 h) Security Forces Act). The question is whether there has been a turn towards an intelligence-led policing (ILP) model.[48] Paraphrasing Lonnie M. Schaible and James Sheffield, we could ask ourselves whether institutional practices within law enforcement have changed in response to homeland security concerns, whether law enforcement agencies have made organizational changes in a manner consistent with ILP, or whether relationships between various tiers of law enforcement have fundamentally changed to

---

[45] *Parejo Alfonso, Luciano*: Seguridad Pública, pp. 50–52. See Royal Decree 952/2018, of 27th July as regards the organisational structure of the Home Department.

[46] Ley Orgánica 2/1986, de 13 marzo, de Fuerzas y Cuerpos de Seguridad.

[47] See also s. 282 CCP, which attributes to the judicial police the mission of ascertaining public offenses that are committed in their territory or demarcation; to practice, according to their powers, the necessary steps to verify them and to discover criminals, and to collect all the effects, instruments or evidence of the crime, making them available to the judicial authority.

[48] Adrian James states that the "true meaning of the term ILP has never really been settled. In Britain, it is confusingly applied to a variety of 'crime-fighting processes that rely on the efforts of analysts and intelligence specialists engaged in crime mapping, crime pattern analysis, data analysis and other problem solving approaches" [*James, Adrian*: Examining Intelligence-Led Policing. Developments in Research, Policy and Practice, Palgrave Macmillan, London, 2013, pp. 1–2]. In the U.S. Lonnie M. Schaible and James Sheffield recall that it "has been widely argued – in the U.S. – that the terrorist attacks on September 11, 2001, revealed critical deficits in [the] nation's homeland defense strategy. Specifically, failure to thwart the attacks using available information has been interpreted as indicating a need for a more comprehensive and strategic coordination of intelligence (Kobach, 2006)". Those authors underline how "[i]ntelligence-led policing (ILP) has been widely advocated as one possible method of overcoming the problems of intelligence sharing and coordination in a post-9/11 world (Ratcliffe, 2008; Cordner and Scarborough, 2010; Carter, 2003; Carter and Carter, 2009). Ratcliffe (2008) proposes that ILP is a business model and managerial philosophy". "Central to ILP –argue these authors– is the utilization of analyzed intelligence to guide decision making and coordination of resources to disrupt and prevent both crime and terrorist threats. Theoretically, this method of policing allows for agencies to more efficiently and strategically target offenders and broader threats through information and intelligence coordinated across agency contexts and with community resources. As such, the principles of ILP identified by Ratcliffe (2008) and others (Carter, 2003; Carter and Carter, 2009; McGarrell et al., 2007) have a strong correspondence with the goals and challenges of post-9/11 policing. Given this, many have advocated the adoption of ILP, poising it for broad diffusion throughout law enforcement". *Schaible, Lonnie M. and Sheffield, James*: "Intelligence-led policing and change in state law enforcement agencies", pp. 761–762.

facilitate the exchange of information and intelligence.[49] At the national level, the Policía and Guardia Civil have specific intelligence units.[50] In the Policía the *Comisaría General de Información*, [General Branch of Information] is in charge of obtaining, receiving and processing information as well as developing analysis of interest in the field of public security and its exploitation for security operations, especially regarding counterterrorist operations related to national and international terrorism.[51] In the Guardia Civil the *Jefatura de Información* [Headquarter of Information] (structured under the command of the Head of Operations) has exactly the same remit.[52] In 2004 the Government approved the creation of the National Counter-Terrorist Coordination Center (Centro Nacional de Coordinación Antiterrorista – CNCA) inside the Home Department (we must recall that 2004 was the year of the Madrid bombings).[53] According to Royal Decree 991/2006, the CNCA was in charge of coordinating and analyzing the information that, in relation to terrorism, both the State Security Forces and the National Intelligence Center had.[54] Originally the plan was for the Guardia Civil and Policía to "lend" 36 agents to the Center, while the terms of the permanent collaboration of the CNI with the CNCA, as well as the agents assigned to the Center, will be the decision of the head of the Defense Department or of the director of the secret services.[55] The same Royal Decree made reference to a new Center, the Intelligence Center against Organized Crime (CICO), also created within the Home Department, to elaborate strategic intelligence in the fight against all types of organized crime, as well as, where appropriate, to establish the criteria for operational coordination of the services acting in that field in the event of

---

[49] Vid. *Schaible, Lonnie M. and Sheffield, James*: "Intelligence-led policing…", p. 762.

[50] The police forces of the autonomous communities also have special intelligence units [see *Llavador Piqueras, Javier and Llavador Cisternes, Hilario*: El régimen jurídico de los servicios de inteligencia en España, pp. 48 ff].

[51] S. 3.2.3 (a) Royal Decree 952/2018, of 27th July, regulating the basic structure of the Home Department [Real Decreto 952/2018, de 27 de julio, por el que se desarrolla la estructura orgánica básica del Ministerio del Interior].

[52] See s. 3 (a) 6 of Royal Decree 952/2018, of 27th July. The first intelligence unit of the Guardia Civil, the Servicio de Información de la Guardia Civil, was created in 1941 and it has evolved to face the new threats that emerged in recent decades [*Hernandez Mosquera, Juan*: "El servicio de información…", pp. 8 and 14–15].

[53] Agreement of the Cabinet of 28th May 2004 [https://www.lamoncloa.gob.es/consejodeministros/referencias/Paginas/2004/c2805040.aspx].

[54] Real Decreto 991/2006, de 8 de septiembre, por el que se desarrolla la estructura orgánica básica del Ministerio del Interior [Royal Decree 991/2006, of 8th September, developing the organisational structure of the Home Department].

[55] See the statement of the Secretary of State for the Home Department [Ministro del Interior] in https://elpais.com/elpais/2004/05/28/actualidad/1085732229_850215.html. The Ertzaintza, the Bask Country police, signed in 2017 a protocol to join the CITCO, a new center which substituted the CNCA (we will deal with this later on) [https://www.elmundo.es/espana/2018/08/27/5b8304d546163fb71f8b45cf.html].

concurrent investigations.[56] Both Centers merged to become the Intelligence Center against Terrorism and Organized Crime [Centro de Inteligencia contra el Terrorismo y el Crimen Organizado (CITCO)].

3. Intelligence and Law Enforcement Techniques and Methods

3.1 The Search for Intelligence using Intrusive Techniques: The Intelligence Service Powers

The CNI is authorized by law to use certain intrusive techniques for gathering intelligence. In 2002 Parliament passed the 2002 Organic Law regulating the previous judicial control of the National Intelligence Center [from now on, the CNI Judicial Control Act] and Act 11/2002, of 6th May, regulating the National Intelligence Center [CNI Act]. The CNI Judicial Control Act lets the CNI take measures that might interfere with the home or communications of individuals in order to fulfill its functions [Single Article of the CNI Judicial Control Act]. The CNI Act, on the other hand, authorizes the CNI to conduct clandestine activities (s. 5.3 CNI Act), though it does not develop it into a more detailed regulation.[57]

Regarding interception of communication and home searches, article 18 SC requires judicial authorization to take such measures (arts. 18.2 and 3 SC).[58] Before

---

[56] S. 2.3.c) of Royal Decree 991/2006, of 8th September. According to this norm the Center will have amongst its tasks:

1. To receive, integrate and analyze as much information and operational analysis related to organized crime as was relevant or necessary for the elaboration of strategic and prospective intelligence in relation to organized crime.

2. To dictate or determine, in the cases of joint or concurrent intervention, the criteria for coordination and action of the operational Units of the State Security Forces, and that of other Intervening Services.

[57] See the distinction between covert action and clandestine activities in *DeVine, Michael E.*: "Covert Action and Clandestine Activities…", p. 1.

«Covert action is codified as an activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States will not be apparent or acknowledged publicly. Covert operations are "planned and executed as to conceal the identity of or permit plausible denial by the sponsor." While not defined by statute, DOD doctrine describes clandestine activities as "operations sponsored or conducted by governmental departments or agencies in such a way as to assure secrecy or concealment" that may include relatively passive intelligence collection information gathering operations […]. This definition differentiates clandestine from covert, using clandestine to signify the tactical concealment of the activity. By comparison, covert operations are "planned and executed as to conceal the identity of or permit plausible denial by the sponsor."»

[58] Article 18. 2: The home is inviolable. No entry or search may be made without the consent of the occupant or a legal warrant, except in cases of *flagrante delicto*. Article 18.

2002 no specific law authorized the intelligence service to carry out interception of communications or search homes. The Code of Criminal Procedure was the only law regulating those measures up until then and referred only to the security forces.[59] Things changed due to a couple of scandals involving the CESID at the end of the 90s. One of those scandals exploded on 12th June 1995 when the newspaper *El Mundo* published that the CESID had been spying on politicians, businessmen and the press without judicial authorization.[60] Even the King had been the object of the interception of communications! Not much later, in March 1998, some members of Herri Batasuna, the political party linked with ETA, discovered that their landline telephone had been intercepted. The agents of the CESID had not asked for judicial authorization in order to intercept those communications.[61] The Audiencia Provincial de Madrid, in the first case, ruled that the CESID activities were against article 18.3 SC, which protects the right to secrecy of communications.[62] It made clear that according to the jurisprudence of the European Court of Human Rights (ECtHR) in the cases *Klass*, *Malone*, *Huvig* and *Kruslin*, the right to privacy as regards communications could only be limited in accordance with the law, that there could be no general or indiscriminate intervention of communications in the name of national security, and that the rule of law implied, *inter alia*, according to *Klass*, that an

---

3. Secrecy of communications is guaranteed, particularly of postal, telegraphic and telephonic communications, except in the event of a court order to the contrary [see https://www.boe.es/legislacion/documentos/ConstitucionINGLES.pdf].

59 Article 579 of the Code of Criminal Procedure (after the implementation of Law nº. 4/1988) allowed a judge to issue an individual warrant to intercept a telephone in the context of a criminal procedure (even during the previous investigatory phase).

60 The CESID had bought some devices in order to protect its radio electric space from, among other things, foreign agents. With the new listening devices they could intercept communications as long as at least one of the persons at one end of the line was using a cell phone. They could not intercept communications that used only corded phones. It was also technically impossible to intercept a specific conversation, since the device scanned a random radio electric frequency. The service justified those interceptions in that the cell phone technology worked with gaps between frequencies and in between the gaps the foreign services could infiltrate and prepare attacks, so they had to oversee those frequencies.

61 The Courts condemned Mario Cantero, an agent of the CESID, to prison, absolving the two directors of the CESID who were in charge of the Center during the years where the interceptions took place [Judgment of the Audiencia Provincial de Álava of 4th April 2003, confirmed by the Supreme Court].

62 Audiencia Provincial de Madrid's judgment 277/1999 (Madrid's Provincial Court Judgment 277/1999). The defendants appealed to the Supreme Court, alleging that the Audiencia Provincial de Madrid had not been impartial, among other issues. In its judgment of 22nd March 2001, the Supreme Court rejected the appeal. The applicants then went to the Constitutional Court, which appreciated a lack of impartiality in the first court (the Audience Provincial) and mandated to repeat the oral judgment. In the new process, the public prosecutor accused just one of the members of the CESID, so the rest of the CESID members who had been condemned in the first place were absolved. The Audiencia Provincial de Madrid, with a new composition, condemned Colonel Perote to four months and a day of prison and six years of suspension for using technical means to intervene communications and record them (Art. 192 bis of the Criminal Code of 1973). The accused appealed again to the Supreme Court, which dismissed the appeal.

interference by the executive authorities with an individual's rights should be subject to an effective control which should normally be assured by the judiciary.

The "new" CNI Judicial Control Act of 2002 empowers the CNI Director to ask the competent Supreme Court Magistrate[63] for authorization to adopt measures that affect not only the secrecy of communications, but also the inviolability of the home as far as those measures are necessary "for the accomplishment of the functions to the Center" (s. 1 CNI Judicial Control Act).[64] The big problem is that the CNI functions are broadly defined by the law, as we have seen. Those missions include obtaining the necessary intelligence to protect and promote the political, economic, industrial, commercial and strategic interests of Spain (s. 4 (a) CNI Act) and preventing, detecting and enabling the neutralization of those foreign services, groups or persons' activities that put at risk, threaten or attack the constitutional order, the rights and freedoms of Spanish citizens, the sovereignty, integrity and security of the State, the stability of its institutions, the national economic interests and the welfare of the population (s. 4 (b) CNI Act). The breadth with which the law delineates the CNI functions implies a different – if not a lower – threshold when assessing the necessity of the measures taken by the CNI than that applicable to the same measures when taken by the security forces.

Under the ECtHR's jurisprudence, "the resultant interference – with the right to privacy – can only be regarded as 'necessary in a democratic society' if the particular system of secret surveillance contains adequate guarantees against abuse". The CNI Judicial Control Act has tried to tie up the powers of the Director of the CNI, asking him to include in its application to the Supreme Court judge in charge of authorizing the measures the following aspects (s. 2, single article CNI Judicial Control Act):

---

[63] Article 342 bis of the Organic Law of the Judicial Power [Ley Orgánica del Poder Judicial] establishes that the Judge authorizing the activities of the National Intelligence Center affecting the fundamental rights recognized in Articles 18.2 and 3 of the Constitution shall be appointed for a period of five years, at the proposal of the General Council of the Judiciary, from amongst Supreme Court judges who have three years of service in the category.

[64] Article 2 (d) of the CNI Judicial Control Act refers to postal, telegraph, telephone or any other kind of communication. The CNI functions are broadly defined by the law, as we have seen. Among its missions, it has to obtain the necessary intelligence to protect and promote the political, economic, industrial, commercial and strategic interests of Spain (s. 4 (a) CNI Act); prevent, detect and enable the neutralization of those foreign services, groups or persons' activities that put at risk, threaten, or attack the constitutional order, the rights and freedoms of Spanish citizens, the sovereignty, integrity and security of the State, the stability of its institutions, the national economic interests and the welfare of the population (s. 4 (b) CNI Act), and secure and defend the Administration against cyber-attacks (s. 4 (e) CNI Act). The breadth with which the law delineates the CNI functions may be a problem when they become the parameter to test the necessity of the measures taken by the CNI (let us remember that under the ECtHR's jurisprudence, "the resultant interference – with the right to privacy – can only be regarded as 'necessary in a democratic society' if the particular system of secret surveillance adopted contains adequate guarantees against abuse").

– Specification of the measures requested.
– Facts that support the application, goals justifying it and reasons that recommend taking those measures.
– Identification of the person or persons affected by the measure if they are known, and designation of the place where it should be practised.
– Duration of the measures, which cannot exceed 24 hours for measures affecting the inviolability of the home and 3 months for the interception of communications. Those periods can be extended for equal periods if necessary.[65]

On the other hand, the CNI Judicial Control Act does not specifically regulate access to data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks, but the Data Retention Act [Act 25/2007 Act, of 18th October, on the retention of data generated or processed in connection with the provision of publicly available lectronic communications services or of public communications networks] authorizes the police forces acting as judicial police and the intelligence services to have access to these data (s. 6.2 a) and c)). In its letter c), s. 6.2 of the Data Retention Act specifies that CNI agents will be given access to the data necessary for the security investigations about persons or premises carried out by the CNI (s. 6.2 c) Act 25/2007). At the same time, the CNI Act establishes that the CNI may conduct these investigations "for the performance of its functions" in the manner provided for in the CNI Act and the CNI Judicial Control Act (s. 5.5 CNI Act). On the other hand, the Data Retention Act (s. 6.1 Data Retention Act) states that a judge must authorize this access. The judicial resolution will determine the data that must be transferred to those authorities "in accordance with the provisions of the Code of Criminal Procedure and respecting the principles of necessity and proportionality" (s. 7.2 Data Retention Act). This provision seems to extend the reference to the Code of Criminal Procedure also to the activities of the intelligence services, which does not make much sense if we take into account that the law refers to security investigations done in the context of intelligence services functions.

The CNI personnel do not have law enforcement powers. The CNI Act states that the CNI personnel "shall not be regarded as agents of the authority, with the exception of those who perform professional tasks related to the protection of the Center's

---

[65] The Act does not establish a maximum total period for this measure once it has been extended, which could run contrary to the proportionality principle. It mandates the Director of the CNI to immediately destroy all the material obtained through these measures if they do not have any relationship with the object or purposes of the said measures (s. 3 of the Single Article of the CNI Judicial Control Act), but it does not contemplate any control measure by the judge in order to oversee that this is really done. A critical analysis of the system of judicial authorization established by the 2002 Organic Law regulating the previous judicial control of the National Intelligence Center, can be found in *De la Oliva Santos, Andrés*: El «control judicial previo».

staff and the Center's facilities" (s. 5.4 CNI Act).[66] The intelligence services cannot intervene or arrest a person if they detect the commission of a crime in the course of their investigations; they have to communicate that discovery to the security forces, who enjoy law enforcement powers.[67]

The Spanish intelligence service adapted its structures to the new democratic order progressively. The Spanish Constitution of 1978 did not include any provision regulating the intelligence services. At the beginning of the new democratic era the legal regime on the intelligence services was formed by different Royal Decrees from the Government. Nonetheless, despite the lack of a global regulation on the intelligence services, it soon became clear that they would not have law enforcement powers. There is no scientific literature in our country theorizing on the reason why the intelligence services were deprived of law enforcement powers in the transition period to democracy, as there is in Germany and other countries. Nonetheless, it is clear that during that period the intelligence services evolved towards a model of service exclusively of an informative nature, targeted to protect national security and subject to the orders of the new democratic Government.[68] In contrast to the old SECED, in charge of suppressing the internal "subversive movements" during Franco's regime,[69] the new intelligence services would be just a piece of the administration, in charge of providing the Government with information and intelligence necessary to prevent any risk or threat affecting the independence and integrity of Spain, the national interest and stability of the rule of law and its institutions (s. 1 CNI Act).[70]

---

66 The State Council [Consejo de Estado], an advisory body with competence to advise on Government bills, considered it necessary to limit the law enforcement powers of the CNI to the protection of staff and the Center's facilities: CNI agents with law enforcement powers could use those law enforcement powers only to that end [Consejo de Estado, Dictamen 3033/2001 (DEFENSA), de 25/10/2001 sobre el Anteproyecto de Ley reguladora del Centro Nacional de Inteligencia (Report 3033/2001 of the State Council, on the National Intelligence Center's Bill)].

67 *Pérez Villalobos, Mª Concepción*: Derechos fundamentales, p. 58.

68 On the history of the first Spanish intelligence service born in the Franco regime and its transformation from an autonomous unit whose goal was to suppress subversive elements towards a modern intelligence service, see *Díaz Fernández, Antonio M.*: Los servicios de inteligencia españoles, pp. 138–208. *Díaz Fernández, Antonio M*: un actor político.

69 See *Díaz Fernández, Antonio M.*: Los servicios de inteligencia españoles, pp. 141 and 177. The SECED had been working in secret since 1968. In 1972 part of its structure was made public but the operative part remained secret [see *ibid*, p. 160].

70 Antonio M. Díaz Fernández distinguishes the role of the intelligence service in a totalitarian regime and in an authoritarian regime. In both totalitarian and authoritarian regimes their mission would be to maintain the security of the regime; so the intelligence would be used against political elites and all those who might be considered to be a security threat. In totalitarian regimes those agencies – says the author – are known as political police. They have a great capacity for penetration into the lives of citizens as they can carry out activities ranging from arbitrary detentions to torture or committing murders. They can decide for themselves as to what poses a threat or not to that regime, because they are entrusted by the Government with the mission of ensuring the security of the regime. Citizens' legal guarantees are non-existent in the face of these organizations. In an authoritarian regime –

3.2 Police Forces Investigating Techniques and Measures

The security forces in Spain (Policía, Guardia Civil and Police Forces of the autonomous communities) play a different role from that of the intelligence services, according to the law, but in order to fulfill their missions, they may also use some of the investigative techniques employed by the intelligence services, though the thresholds that may trigger the adoption of such measures are different in each case.

The missions of the security forces, as we already have seen, are on the one hand the protection of individuals from dangers to their basic rights and freedoms; that is, they are in charge of the maintenance of public security and the prevention of crimes – 104 SC – (*Gefahrabwehr* in German), and, on the other hand, to contribute to the investigation of crimes under the instruction of judges or the public prosecutor – 126 SC – (*Strafverfolgung* in German).[71]

Security forces agents are considered as having authority to perform law enforcement actions.[72]

---

according to this author – the intelligence services act as independent security agencies. They often base their activity on disabling threats through their knowledge so their degree of penetration is much lower than on totalitarian regimes. This is how, for example, files are created in which public and private life data are collected to use them in the future. Both organizations have in common their high degree of autonomy from the state's elites. In totalitarian regimes the intelligence service may even «suppress» individuals appertaining to those elites if they consider that they depart from the principles and ideology of the regime. In authoritarian regimes the intelligence service are always accountable to a part of the elite of the state; however, they decide who are active subjects of anti-regime activities and how to fulfill their duties at their own discretion [free translation of *Díaz Fernández, Antonio M.*: un actor politico, p. 202].

[71] S. 11 of the Organic Law 2/1986, of 13th March, on Security Forces says the following: Article 11

1. The mission of the State Security Forces is to protect the free exercise of rights and freedoms and to ensure citizen security through the performance of the following functions:
(a) Ensure compliance with the Laws and general provisions.
(b) Assist and protect persons and ensure the preservation and custody of property that is at risk for any cause.
(c) Monitor and protect public buildings and facilities.
(d) Ensure the protection and safety of high personalities.
(e) Maintain and restore, where appropriate, order and citizen security.
(f) Prevent the commission of criminal acts.
(g) Investigate crimes to uncover and detain alleged culprits, to secure the instruments, effects and evidence of crime, making them available to the competent Judge or Court, and to prepare technical and expert reports from them.
(h) Capture, receive and analyze as much data as are of interest to public order and security, and study, plan and execute crime prevention methods and techniques.
(i) Collaborate with the Civil Protection Services in cases of serious risk, catastrophe or public calamity, in the terms established in the Civil Protection legislation.

[72] S. 7 Organic Law 2/1986, of 13th March, on Security Forces.

The security forces have the following powers in connection with the maintenance of public security and the prevention of dangers[73]:

– Enter and search homes (including business premises) and official premises (s. 15 Organic Law 4/2015, of 30th March, on the Protection of Citizen Security).
– Identify those who have infringed the law (stop them in order to identify them). The security forces also have the power to identify someone when it is necessary to prevent a crime (s. 16.1 Organic Law 4/2015).
– Search a person when there are reasonable grounds to believe that it may lead to the discovery of instruments, effects or other objects relevant to the exercise of its functions of inquiry and prevention (s. 20 Organic Law 4/2015).
– Limit or restrict the movement of people in public places and establish security zones in cases of alteration of citizen security or peaceful coexistence.[74] The security forces may also preventively seize any effects or instruments likely to be used for illegal actions (s. 17 (1) Organic Law 4/2015).
– Establish controls on public roads, public places or establishments to stop and register vehicles or control personal effects in a superficial manner (s. 17 (2) Organic Law 4/2015).[75]
– Practice checks on persons, goods and vehicles on public roads, public places and establishments when it is necessary to prevent the illegal use of weapons, explosives, dangerous substances or other objects, instruments or means which generate a serious risk for people or which are likely to be used for the commission of a crime or to alter public safety, whenever there is a sign of their eventual presence in such places, proceeding, where appropriate, to seize them (ss. 18 (1) and 18 (2) Organic Law 4/2015).
– Protect people at meetings and demonstrations, preventing public safety from being disturbed (s. 23 (1) Organic Law 4/2015).
– Dissolve public meetings and demonstrations in the cases provided for in article 5 of Organic Law 9/1983 of July 15, regulating the right of assembly, and remove vehicles and other obstacles when they endanger or hinder movement in public spaces (s. 23 (1) Organic Law 4/2015).

---

[73] Here we will just refer to the powers of the state security forces, not to those from the autonomous communities' security forces.

[74] When there are rational grounds that indicate that this alteration may occur, they can limit or restrict the circulation of people just while it is necessary for the maintenance or restoration of security (s. 17.1 Organic Law 4/2015).

[75] Those measures can only be taken if they are essential for the prevention of serious crime or of crimes which generate social alarm, or for the discovery and detention of those who have taken part in the commission of such crimes and for the collection of instruments, effects or evidence of those crimes (s. 17 (2) Organic Law 4/2015).

As *Policía Judicial* (*Strafverfolgung*),[76] the security forces may:

– Act under a fake identity (undercover) in order to investigate activities of organized crime with the authorization of a judge or the public prosecutor, giving in such circumstance immediate account to the judge (s. 282 *bis* (1)).[77]
– Act undercover in closed communication channels in certain circumstances enumerated in section 282 *bis* (6) with a judicial warrant.
– Arrest an individual in the circumstances described in s. 492 of the Code of Criminal Procedure [CCP].[78]
– Enter and search homes with a warrant (s. 550 CCP).[79]
– Intercept private written postal or telegraphic correspondence usually with a judicial warrant (s. 579 CCP).[80]

---

[76] According to the Code of Criminal Procedure [CCP] – article 282 – the *Policía Judicial*'s mission is investigating crime and bringing offenders to justice, taking the necessary steps to discover the offenders, and to collect all the effects, instruments or evidence of the crime, making them available to the judicial authority.

[77] In their undercover activity, the security forces are authorized to acquire and transport objects, effects and instruments of the crime and to defer their seizure (s. 282 *bis* (1)). The alleged identity will be granted by the Ministry of the Interior for a period of six months extendable for periods of equal duration, being the security forces legitimately empowered to act in everything related to the specific investigation and to participate in legal and social traffic under such identity.

[78] According to section 553 CCP police officers may immediately proceed to arrest persons by their own authority where there is a prison order against them, when they are caught in *flagrante delicto*, where an offender, immediately prosecuted by the agents, hides or shelters in a house. In cases of exceptional or urgent need, they are allowed to arrest those who have committed the crimes described in article 384 *bis* (terrorism) wherever they are hidden or sheltered, as well as search the place and seize the effects and instruments found therein which could relate to the offense pursued (s. 553 CCP).

[79] The investigating judge may issue a search warrant authorizing the entry, day or night, if urgency so requires, when there is a sign that the defendant or effects or instruments of the crime are there, or there are books, papers or other objects that may serve to discover or prove the crime (s. 550 CCP). The judge may also issue a warrant authorizing the security forces to enter public buildings for the same reasons, day or night [s. 546 CCP]. The judge shall not order the search of record books and accounting papers of the defendant or another person unless there is serious evidence that this diligence will result in the discovery or proof of any material facts or circumstances of the case (s. 573 CCP).

[80] The judge would issue the warrant if there is evidence that it will serve to discover or prove any event or circumstance relevant to the case, provided that the investigation concerns any of the following offenses: 1. Malice offenses punishable by imprisonment with a maximum limit of at least three years in prison. 2. Crimes committed within a criminal group or organization. 3. Terrorism offenses (s. 579.1 CCP).

In case of urgency, where investigations are carried out for the investigation of crimes related to the action of terrorist elements and there are reasonable grounds to believe that the measure is essential, it may be ordered by the Minister of the Interior or, given the case, by the Secretary of State for Security. This measure shall be communicated immediately to the competent court, at the most within a maximum period of twenty-four hours, stating the reasons justifying the adoption of the measure, the actions taken, the manner in which it has been carried out and its outcome. The competent court shall, in a reasoned manner, revoke

– Intercept telephone and telematics communications usually with a judicial warrant (s. 588 *ter* a) to i) CCP).[81]
– Access traffic data or data associated to the communication with a judicial warrant (s. 588 *ter* j) CCP).
– Identify terminals by capturing identification codes of the device or of its components (s. 588 *ter* l)).
– Collect and record direct oral communications maintained by the person being investigated, in public or open spaces, or at home or in any other enclosed place with a judicial warrant (s. 588 *quater* a) CCP). If the judge authorizes it, the security forces may also take pictures.
– Obtain and record images of the investigated person when he is in a public place by any technical means, if it were necessary to facilitate his identification, to locate the instruments or effects of the crime or to obtain relevant data to the clarification of the facts (s. 588 *quinquies* a) CCP).
– Use devices or technical means of monitoring and location with a judicial warrant (s. 588 *quinquies* c) CCP).
– Access the content of computers, telephone or telematics communication instruments or mass storage devices or telematics data repositories with a judicial warrant (s. 588 *sexies* a) to c) CCP).
– Use identification data and codes, as well as the installation of software to search remotely the contents of a computer, electronic device, computer system, mass storage device or database with a judicial warrant (s. 588 *septies* a) to c) CCP).

Regarding the powers of the security forces to *enter and search people's houses or private premises*, the security forces will not need a warrant if they have obtained the permission of the person concerned or in cases of *flagrante delicto*.[82] The need to avoid imminent and serious harm to persons and things in cases of catastrophe, calamity, imminent ruin or similar extreme and urgent cases are also legitimate causes for entry into a home by the security forces (s. 15 (2) of Organic Law 4/2015). If none of these circumstances are present in the particular case, the security forces will

---

or confirm such action within a maximum period of seventy-two hours after the measure was ordered (s. 579.3 CCP).

[81] In case of urgency, where investigations are carried out for the investigation of crimes related to the action of terrorist elements and there are reasonable grounds to believe that the measure is essential, it may be ordered by the Minister of the Interior or, given the case, by the Secretary of State for Security. This measure shall be communicated immediately to the competent court, at the most within a maximum period of twenty-four hours, stating the reasons justifying the adoption of the measure, the actions taken, the manner in which it has been carried out and its outcome. The competent court shall, in a reasoned manner, revoke or confirm such action within a maximum period of seventy-two hours after the measure was ordered (s. 588 *ter* d) 3 CCP).

[82] Article 18.2 SC says that no entry or search may be made at homes without the consent of the occupant or a legal warrant, except in cases of *flagrante delicto*.

need a judicial warrant in order to enter and search private premises. The investigating judge may issue a search warrant authorizing the entry into the home or private premises, day or night, if urgency so requires, where there is evidence that the defendant or effects or instruments of a crime are there, or there are books, papers or other objects that may serve to discover or prove a crime (s. 550 CCP).[83] The judge may also issue a warrant authorizing the security forces to enter public buildings for the same reasons, day or night (s. 546 CCP). Regarding the threshold to allow such measures, the Constitutional Court has asked the judge to evaluate the severity of the facts allegedly investigated.[84] The Court does not deem it necessary to cement the judicial resolution in a rational indication of the commission of a crime; for the Court a *notitia criminis* will suffice, supported by a suspicion founded on objective circumstances (evidence) that a crime could have been committed, or is being committed or will be committed [vid. Judgment of the Spanish Constitutional Court 136/2000, § 4].[85]

The security forces can *search mail or the telegraphic correspondence* but they will need a judicial warrant.[86] The judge may authorize that measure where there is evidence that a relevant fact or a relevant circumstance for the criminal prosecution will be discovered or verified, but only in cases concerning crimes committed with malice and punished with a maximum penalty of at least three years' imprisonment, or crimes related to organized crime or terrorism (s. 579.1 CCP).

The security forces can also *intercept telephone and telematics communications* in the context of a criminal procedure. The judge must specify in the warrant

---

[83] The judge shall not order the search of record books and accounting papers of the defendant or another person unless there is serious evidence that this diligence will result in the discovery or proof of any material facts or circumstances of the case (s. 573 CCP).

[84] The judge must motivate his resolution, indicating the reasons for authorizing such a measure; he must take into account whether the investigation comes from a judicial instruction initiated in advance or from a mere police activity which is the origin, precisely, of the criminal instruction.

[85] The measure must pursue a constitutionally legitimate aim [judgment of the Spanish Constitutional Court 171/1999, 27th September, § 10 and judgment 41/1998, § 34] and it must respect the principle of proportionality [vid. Judgment of the Spanish Constitutional Court 197/2009, 28th September, § 8]; the search must be appropriate and essential to attain the legitimate aim [vid. Judgments of the Spanish Constitutional Court 55/1996, 161/1997, 61/1998, 171/1999, § 10]. When the judge authorizes the entry and registration of a home, in the context of a criminal procedure, he or she has to express in detail the judgment of proportionality of the limitation imposed, the spatial (location of the home) and temporary circumstances (moment and time) of the entry and registration, and if possible also the personal elements of the resolution (owner or occupant of the domicile in question) [Judgments of the Spanish Constitutional Court 181/1995, 11th December, § 5; 290/1994, § 3; Resolution of the Constitutional Court 30/1998, 28th January, § 4].

[86] The Home Secretary (*Ministro del interior*) or Home Undersecretary (*Secretario de Estado de Seguridad*) might authorize that measure in urgent cases, communicating it immediately to the judge (maximum time limit twenty-four hours), but only where the investigation concerns organized crime or terrorism. The judge will have to confirm or revoke such measure in no more than seventy-two hours since the measure was taken (s. 579.3 CCP).

authorizing the interception the data or facts that may be considered as evidence to the existence of a crime and the connection of the person or persons investigated with it;[87] indications of a crime must be more than mere suspicions (Judgments of the Constitutional Court 167/2002, of 18th September, § 2; 184/2003, of 23rd October, § 11; and 197/2009, of 28th September, § 4). There must be a real basis from which it can be inferred that the offense has been committed or will be perpetrated [Judgment 150/2006, 22nd May]. That evidence must be more than just suspicions, but can be less than the rational indications required for processing someone.[88] The Court excludes purely prospective research based on the generic need to prevent or discover crimes or to clear suspicions without an objective base (see also, Judgment of the Constitutional Court 253/2006, §2).[89] The judicial warrant must be based on objective data that can be considered evidence of the possible commission of a serious crime and of the connection of persons affected by the intervention to the facts investigated.[90] The law has reserved this measure to the investigation of the crimes enumerated in s. 579.1 CCP, adding also to them those crimes committed through computers or any other technological device or using a communications service. The application for a warrant may ask the judge to authorize access to the content of the conversation or to the traffic data, location data and the related data necessary to identify the subscriber or user of the communication (s. 588 *ter* 2) CCP).[91]

---

87 When a judge authorizes the interception of communications or extends the authorization for a new period, he or she must specify all the essential elements to carry out the judgment of proportionality and to make the subsequent control of the measure possible, in order to respect the right of defense of the person subject to the measure (STC 145/2014, § 2).

88 STS 377/2013, 13th February 2013 [ECLI: ES:TS:2013:377], reproducing also the jurisprudence of the Constitutional Court or STS 376/2018 [ECLI: ES:TS:2018:3093] *inter alia.*

89 In 2015 the Code of Criminal Procedure was amended [Organic Law 13/2015 amending the Code of Criminal Procedure in order to strengthen the procedural guarantees and regulate technological investigative measures) of 5th October 2015]. The new s. 588 *bis* a) CCP demands that the measure be taken for the investigation of a particular crime and forbids the use of those measures to prevent or uncover crimes or to clear suspicions without an objective basis. S. 588 *bis* a) CCP is a common provision applicable to the interception of telephone and telematics communications, the collection and recording of oral communications through the use of electronic devices, the use of technical devices for monitoring and capturing images, the search of mass storage devices, and remote searches on computer equipment.

90 The inclusion of a crime in the category of serious crimes will depend not only on the penalty assigned to the offense but also on the harm to the legal good or interest protected by the norm and the social relevance of the offense [see, among others, judgments of the Spanish Constitutional Court 104/2006, 3rdApril, §3; 166/1999 of 27th September, § 3(a)], 299/2000, 11th December, §2). On the jurisprudence of the Constitutional Court related to this point and the discussion of the meaning of serious crime before the approval of the Organic Law 13/2015, of 5th October amending the Code of Criminal Procedure in order to strengthen the procedural guarantees and regulate technological investigative measures, see *López-Barajas Perea, Inmaculada*: La intervención, pp. 110–114.

91 The Home Secretary (*Ministro del interior*) or Home Undersecretary (*Secretario de Estado de Seguridad*) might authorize that measure in urgent cases communicating it

Regarding *access by the security forces to data retained according to the Data Retention Act* [Act 25/2007, of 18th October], the law establishes the necessary authorization by a judge (s. 6.1 Data Retention Act). According to s. 588 *ter* j) CCP "where knowledge of those data is essential for the investigation, application must be made to the competent court for authorization to access the information in the automated archives of the service providers, in particular for the purpose of a cross search or a smart search of the data, provided that the nature of the data of which it is necessary to have knowledge and the reasons justifying the communication of those data are specified". The judge in its resolution must respect the principles of necessity and proportionality (s. 7.2 Data Retention Act & s. 588 *bis* a) CCP).[92] As to the threshold for authorizing this measure, the key element is that of proportionality. There is no list of crimes whose investigation triggers the authorization of this measure by a judge. The Audiencia Provincial de Tarragona (Provincial Court, Tarragona, Spain) asked for a preliminary ruling to the European Court of Justice (ECJ) in relation to article 15 of the Directive 2002/58 and articles 7 and 8 of the Charter, as interpreted by the Court in its judgment of 8th April 2014, *Digital Rights Ireland and Others*, and in *Tele2 Sverige and Watson and Others* in order to see if that measure could only be ordered where the investigation was related to serious crimes.[93] In its answer to the preliminary ruling the ECJ holds that "in areas of prevention, investigation, detection and prosecution of criminal offenses, only the objective of fighting serious crime is capable of justifying public authorities' access to personal data retained by providers of electronic communications services which, taken as a whole, allow precise conclusions to be drawn concerning the private lives

---

immediately to the judge (maximum time limit twenty-four hours), but only where the investigation concerns organized crime or terrorism. The judge will have to confirm or revoke such measure in no more than seventy-two hours since the measure was taken [s. 588 *ter* d) 3 CCP].

92 Judicial police officers are allowed to obtain the identification codes or labels of telecommunications devices or any of their components, such as the IMSI or IMEI number, and in general, of any technical element that identifies the communication equipment used or the SIM card used to access the network without a judicial warrant, using technical devices, as long as it would not have been possible to obtain the number necessary for the purposes of the investigation during the investigation. Once the codes that allow the identification of the appliance or any of its components have been obtained, those judicial police officers may request the intervention of communications from the competent judge in the terms set out in article 588 *ter* d) CPP. The request mentions the use of the artifices referred to in the preceding paragraph to identify the device (s. 588 *ter* l) CCP). This "power" was first regulated in Organic Law 13/2015, but had been recognized before by the jurisprudence of the Supreme Court [*inter alia* STS 377/2013 (ECLI: ES:TS:2013:377); STS 249/2008 (ECLI: ES:TS:2008:2756)]. In its jurisprudence the Court says that this access to the IMSI does not affect the secrecy of the communications (which is subject to judicial warrant by the Spanish Constitution), but to other aspects of privacy, such as the right to be left alone ("derecho a la intimidad") in connection with the protection of the individual with regard to the processing of personal data.

93 See judgment of the European Court of Justice (Grand Chamber) in Case C-207/162, 2nd October 2018 [ECLI:EU:C:2018:788], § 50.

of the persons whose data is concerned (see, to that effect, *Tele2 Sverige and Watson and Others*, paragraph 99)". But "when the interference that such access entails is not serious, that access is capable of being justified by the objective of preventing, investigating, detecting and prosecuting 'criminal offenses' generally."[94]

The security forces, as the intelligence services, can *act undercover*.[95] The Code of Criminal Procedure in its article 282 *bis* limits the context in which the security forces can act undercover to the fight against organized crime.[96] The competent Judge of Instruction or the Public Prosecutor's Office (giving immediate account to the Judge) may authorize an agent to act undercover taking into account the need for the purposes of the investigation (s. 282 *bis* 1) CCP).[97] The Supreme Court has clarified that the measure is taken in investigations related to organized crime, that is, police inquiries obviously already underway. It is the certain quality of the information already in the hands of the police that provides the foundation to authorize the measure, which, obviously, says the Supreme Court, because of its extraordinary nature, could only be adopted in view of clear data.[98]

The law regulating the intelligence services has not been updated, unlike the Code of Criminal Procedure. Therefore, in that law there is no reference to such powers as that of collecting and recording direct oral communications maintained by certain

---

[94] *Ibid*, §§ 54 & 57. A critical analysis of this judgment of the ECJ can be found in *Oubiña Barbolla, Sabela:* La proporcionalidad…", pp. 303–335; *Rodríguez Lainz*, *José Luis*: "El Régimen Legal español…", pp. 1–12.

[95] The intelligence services agents are not agents of the authority nor do they hold functions of judicial police power that legitimizes them to obtain evidence for the criminal process or to establish the facts investigated [*Expósito López, Lourdes*: El agente encubierto, p. 262].

[96] Section 282 *bis* 4) CCP enumerates the crimes considered to be organized crimes to this effect. A crime will be organized if it includes the association of three or more persons to carry out the following offenses: (a) Illicit trafficking of human organs and transplantation thereof; (b) Abduction of persons; (c) Trafficking in human beings; (d) Prostitution offenses; (e) Anti-equity and socio-economic offenses; (f) Intellectual property offenses; (g) Offenses against workers' rights; (h) Crimes against the rights of foreign nationals; (i) Trafficking in endangered species of flora or fauna; (j) Trafficking in nuclear and radioactive material; (k) Public health offenses; (l) Counterfeiting of currency and forgery of credit or debit cards or travelers' checks; (m) Trafficking and deposit of arms, ammunition or explosives provided for in articles 566 to 568 of the Penal Code; (n) Terrorism offenses; (o) Historical heritage offenses.

The CCP also authorizes the investigating judge to authorize judicial police officials to act under a false identity in communications held in closed communication channels in order to clarify any of the offenses referred to in paragraph 4 of s. 282 *bis* CCP or any offense provided for in s. 588 a) CPP. To act as an "online undercover agent" the authorization of a judge is always necessary.

[97] The Code of Criminal Procedure specifies that where their acts may affect fundamental rights, the undercover agent shall request authorization from the competent judicial body in the terms established by the constitution and the law.

[98] STS 277/2016, 6th April; STS 682/2019, 28th January [ECLI: ES:TS:2020:207].

individuals,[99] that of recording images, the power to use spy software to search remotely the contents of a computer or electronic device,[100] or the power to access the content of computers[101] – though in this last case, the Supreme Court jurisprudence on the search of goods found in a house or premises being searched with a judicial warrant would be applicable, but the cases where the computer is not seized at a home search would not be included and therefore would lack any regulation regarding the intelligence services.[102]

4. Coordination between Police Forces and the CNI

As we saw in the first part of this analysis, there are common threats confronting the CNI and the police forces. The CNI must prevent, detect and enable the neutralization of those foreign services, group or individual activities that put at risk, threaten or attack the *constitutional order, **the rights and freedoms of Spanish citizens**, the sovereignty, integrity and security of the State, the stability of its institutions, the national economic interests and the welfare of the population* (s. 4 (b) CNI Act). The police forces must protect the free exercise of the rights and freedoms of citizens and guarantee their security.

---

[99] The Constitutional Court in its judgment STC 145/2014, 22nd September said that the old Code of Criminal Procedure did not offer sufficient legal basis for the police to adopt such measures, specifying that the provisions regulating the intervention of the communications weren't applicable to that kind of measure. The CNI Act and the CNI Judicial Control Act only regulate the interception of communications but say nothing on the direct recording of conversations.

[100] Section 588 *septies* a) CCP indicates that the judge may authorize the use of identification data and codes, as well as the installation of software, which allow remote examination of the contents of a computer, electronic device, computer system, mass storage instrument of computer data or database without the knowledge of its owner or user provided that it pursues the investigation of any of the following crimes: (a) Crimes committed within criminal organizations; (b) Terrorism offenses; (c) Crimes committed against minors or persons with judicially modified capacity; (d) Crimes against the Constitution, treason and relating to national defense; (e) Crimes committed through computer tools or any other information technology or telecommunication or communication service.

[101] According to the jurisprudence of the Constitutional Court and the Supreme Court, police forces need a judicial warrant to get access to the contents of any computer except for urgent cases. The judge must take into account the proportionality principle when authorizing the measure [STC 173/2011, 7th November; STS 342/2013, 17th April; STS 462/2019, 14th October].

[102] Remote access to computers by the police can only be authorized in connection with the following crimes: (a) Crimes committed within criminal organizations; (b) Terrorism offenses; (c) Crimes committed against minors or persons with judicially modified capacity; (d) Crimes against the Constitution, treason and relating to national defense; (e) Crimes committed through a computer or any other information technology or telecommunication or communication service (s. 588 *septies* a) CCP).

In 2015 the Government passed the first National Security Act (previously there were different laws regulating national defense and the Armed Forces).[103] The Act considers that national defense, public security and external action are fundamental components of national security. It asks the CNI to permanently support the National Security System, providing elements of judgment, information, analysis, studies and proposals necessary to prevent and detect risks and threats and to contribute to their neutralization, within the scope of its powers (s. 9 National Security Act). The Act names some special areas of interest to national security which include cybersecurity, economic and financial security, maritime safety, air and outer space security, energy security, health security and environmental preservation (s. 10 National Security Act). Public Administrations with competence in these areas of special interest are obliged by law to establish mechanisms for coordinating and sharing information, and alert systems in the case of possible risks and threats (s. 11 National Security Act).[104]

Both the police and the CNI have powers in the field of cybersecurity. Cyberattacks are an important threat to national security – a threat that must also be confronted by the intelligence services and the police forces, according to the 2011 National Security Strategy. Cyberattacks threaten critical infrastructures and serve as a means for other states, terrorists or other kinds of criminals to spy on our country. The most common attacks according to this 2011 Strategy were those directed against commercial targets. The protection against this threat is said to come from multiple actors, including the CNI, through the Centro Criptológico Nacional (CCN) [National Cryptographic Center], the Armed Forces, and the Centro de Protección de Infraestructuras Críticas (CNPIC) [Critical Infrastructure Protection Center].[105]

---

[103] National Security Act 36/2015 [Ley 36/2015, de 28 de septiembre, de Seguridad Nacional].

[104] There is a Delegated Commission of the Government called the National Security Council, which assists the Prime Minister in all that has to do with National Security Policy. The Commission is formed of the Prime Minister, the Vice President, the Secretaries of State (*Ministros*) of Foreign Affairs and Cooperation, Justice, Defense, Finance and Public Administration, Home Department of Industry, Energy and Tourism, of Presidency, of Economy and Competitiveness and of Health, Social Services and Equality, the undersecretaries of state of Foreign Affairs and Security, the director of the Prime Minister cabinet director, the Chief of Staff of the Armed Forces and the Director of the CNI (s. 21.3 National Security Act). Article 21.1 National Security Act details the functions of this Commission.

[105] Estrategia de Seguridad Nacional (2011), pp. 65–67. The Strategy remarks that espionage has adapted to the new security scene, taking advantage of the possibilities offered by the new information and communication technologies and the globalization process. The Strategy maintains that intrusions into cyberspace to get information are becoming more common and troubling. Of particular importance is economic espionage, consisting of the illicit acquisition of information, patents or critical technologies, and even in the illegal influence of political decisions of an economic nature. Its potential impact is increasing because of its ability to damage the economic system and affect the well-being of citizens, the Strategy indicates. Espionage continues to be a real and evolving threat. The Strategy says we must face the activities of foreign intelligence services, groups or people that threaten the rights, freedoms and well-being of Spanish citizens, the sovereignty, integrity and

This CNPIC is a ministerial body responsible for the boost, coordination and supervision of all the activities entrusted to the Secretary of State for security (the chief of the police forces) in relation to the protection of critical infrastructures in the national territory.[106] Here there seems to be two different bodies covering the same field, but the question is, are there instruments to foster the coordination of CNI and police forces? And, do they really intertwine or act together in any particular field?

We cannot look for the answer in the Intelligence Directive, as it is secret, neither can we go through parliamentary reports on the CNI to try to answer this question, as they are non-existent, in contrast to what happens in other countries. The only way to answer this question is to find indirect ways to do it, for example going through other reports – like the National Security Strategy, first published in 2011 – or surfing the content of the law or the CNI webpage.

The National Security Strategy, first published in 2011, stresses the need for internal and international coordination in order to preserve security. It underlines the necessity to promote an interdisciplinary and integrated vision of security in the 21st Century.[107]

The CNI Act mandates the National Intelligence Center to maintain, "with the rest of the public Administrations, the relations of cooperation and coordination necessary for the better fulfillment of its missions, in accordance with the legislation in force in each case and preserving the legal protection of the activities of the Center" (s. 5.2 CNI Act).

In 2002 the CNI Act, for the first time, provided for a governmental Delegate Commission of Intelligence, whose tasks would include the coordination of the intelligence activity of the CNI with that of the information services of the police forces and the intelligence units of the civil and military administration in order to create an intelligence community (ss. 6.1 and 6.3 CNI Act).[108] This commission is led by the vice-president and formed by the Foreign Affairs Secretary (Ministro de Asuntos Exteriores), Home Secretary (Ministro del Interior), Defense Secretary (Ministerio de Defensa), Economy Secretary (Ministro de Economía), the Secretary General of

---

security of the State, the stability of their Institutions or national interests. To that end, Spain will enhance the capacities of intelligence and counterintelligence of the State, both at the technological and human level [Estrategia Española de Seguridad (2011), p. 69].

106 Artículo 7 de la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas (s. 7 of the 8/2011 Act of 28th April, establishing measures in order to protect the critical infrastructures). The Constitutional Court links cybersecurity to the necessary actions of prevention, detection and response to the cyber threats, affecting issues related to public safety and defense [Judgment of the Constitutional Court 142/2018, from 20th December (STC 142/2018, de 20 de diciembre (ECLI:ES:TC:2018:142)].

107 Estrategia Española de Seguridad (2011), p. 9.

108 The principle of coordination is already recognized by the Spanish Constitution as one of the principles guiding the functioning of the administration (Art. 103 SC).

the Presidency, the Undersecretary of Security (Secretario de Estado de Seguridad) and the Undersecretary of the CNI (Art. 6.2 CNI Act).[109]

According to the CNI Act the Delegate Commission of Intelligence has, in fact, two different functions. First, to propose the annual objectives of the CNI to the president and to control the accomplishment of those objectives by the CNI (Executive oversight of the CNI).[110] The second task of the commission is, as already said, to look after the coordination of the CNI with the police forces and the organs of the civil and military administration relevant to fulfill intelligence goals. The coordination between the police forces and the CNI through the Delegate Commission is done at the very top political level. The Delegate Commission is concerned mainly with general issues and joint proposals, not with particular operations, as far as we can derive from its regulation.[111] On the other hand, the law obliges the CNI director to keep and develop the necessary collaboration with the information services of the police forces and the civil and military administration, being mindful of intelligence goals [s. 9 d) CNI Act].

The collaboration between the CNI and the police forces is close in the fight against terrorism and organized crime. Concerning terrorism, we have already explained how the Spanish intelligence services played an important role in the fight against ETA and have referred to the creation in 2001 of a new unit inside our intelligence services focused on international terrorism. The first National Security Strategy of 2011 also underscored the important role of the police forces and the intelligence services in the fight against ETA and, recently, in the fight against international terrorism. It referred to the increment of material, economic and human resources devoted to the antiterrorist units of the Policía and the Guardia Civil (those bodies' personnel grew 40% from 2004 until 2011, year of the publication of the Strategy). The strategy gave notice of the creation of an antiterrorist police network working in foreign countries. The CNI was strengthened in order to counter the

---

[109] The Commission has the possibility to call other directive members of the administration to the meetings (s. 6.3 CNI Act).

[110] Until 2011, the CNI itself proposed the intelligence objectives to the Delegate Commission. Since 2011, different administrative bodies share their needs with the CNI and the CNI elaborates a draft of the Intelligence Directive that submits to the Delegate Commission. It is for the Delegate Commission to propose the CNI objectives to the Prime Minister and it is for the Government to approve them (ss. 3 and 6.4 (a) CNI Act). The Intelligence Directive gathers around 20 intelligence goals every year [see https://www.europapress.es/nacional/noticia-nueva-directiva-inteligencia-cni-elabora-colaboracion-primera-vez-organismos-estado-20101122145342.html].

[111] According to the law, Delegate Commissions can have the following functions: (a) to examine general issues relating to several ministerial departments; (b) to study those matters which, affecting several ministries, require the elaboration of a joint proposal prior to its resolution by the Council of Ministers; (c) to resolve matters which, affecting more than one ministry, do not need to be elevated to the Council of Ministers; (d) to exercise any other attribution conferred on them by the legal system or delegated to them by the Council of Ministers (s. 6 (4) 1997 Government Act; Ley 50/1997, de 27 de noviembre, del Gobierno).

terrorist threat. Informative and operation collaboration with equivalent foreign services had been boosted, according to the strategy.[112] The CNI budget for the 2017 exercise was increased by 8.3% – from € 240,980,000 in 2016 to € 260,960,000 in that year – specifically to reinforce the fight against international jihadi terrorism and cybersecurity. The Government justified this increase because the objective was to equip the CNI with the necessary tools "to prevent and avoid any risk and threat". To this end, the Government authorized the secret services to incorporate 600 new officials in the following five years.[113]

Amongst the measures to fight terrorism, the Strategy includes the "principle of immediate availability of data about information and antiterrorist intelligence" (sic) and the creation of the Centro Nacional de Coordinación Antiterrorista (CNCA) – Antiterrorism National Coordination Center – with the participation of the police forces, the CNI and the penitentiary administration. The Center would collaborate with the autonomous communities' police forces, and other EU and international allies.[114] The CNI webpage informs that "the CNI has a counterterrorism division, which works on both national and non-national terrorism", and adds that "the fight against terrorism is one of the highest priority objectives entrusted to the Center" and that "the CNI participates in the National Center for Counterterrorism Coordination (CNCA) through the integration of some of its staff in the Center" and by way of sharing with the Center intelligence reports on terrorism.[115]

The Home Department said the Center would be a joint and permanent police unit, not an operations unit, with its own headquarters composed of members of the Policía and the Guardia Civil and the participation of the CNI. The Center functions would include the reception, treatment and strategic analysis of terrorism-related information. Members of the Center, according to press releases, would have direct access to the police and intelligence databases, assess risks and threats to Spain, and propose and plan, where appropriate, joint responses to terrorist threats.[116]

---

[112] Estrategia Española de Seguridad (2011), pp. 49–51. In 2005 the Parliamentary Commission of the 11/M (11th March, the day of the terrorist attack to the trains in Madrid, in 2004) concluded that the Policía, the Guardia Civil and the CNI should see their human resources tripled in its central units [https://www.20minutos.es/noticia/9491/0/comision/11-M/pp/].

[113] https://okdiario.com/investigacion/cni-dice-rajoy-obvio-alerta-eeuu-atentado-70-asi-ano-1299444

[114] After the terrorist attacks of 11th March 2004 in Madrid, the Government created the National Center of Antiterrorist Coordination [Centro Nacional de Coordinación Antiterrorista (CNCA)]. The Center was created on the 28th May 2004. There is some resemblance with the NCTC in the USA or the JTAC in the UK, but the Spanish CNCA had a less operative focus. *Díaz Fernández, Antonio M.*: Teoría de las organizaciones, p. 37.

[115] https://www.cni.es/es/preguntasfrecuentes/pregunta_004.html?pageIndex=4&faq=si&size=15 [searched on 15th March 2019].

[116] http://www.interior.gob.es/noticias/detalle/-/journal_content/56_INSTANCE_1YSSI3xiWuPH/10180/1170666/

The CNCA was finally created by Agreement of the Council of Ministers of 28th May 2004. In 2012, the CNCA was placed under the oversight of the Undersecretary of State for Security (Home Department), with the double aim of reinforcing coordinating tasks and maximizing the use of information that this Center collects and processes.[117]

In 2007 the Secretary of State for the Home Department announced the creation of a complex computer structure at the CNCA that would collect data of all ongoing investigations carried out by the Policía, Guardia Civil and National Intelligence Center (CNI) to avoid duplications and thus avoid discoordination between the different bodies. It would highlight coordination methods in operations where this was suitable. The objective of the system would be to collect and analyze information, evaluate risks and make operational and strategic recommendations, according to the Secretary of State for the Home Department.[118] The anti-terrorist Operations Cooperation System (SICOA) – the database – would follow the investigations of the Policía, Guardia Civil and the CNI.[119]

The Strategy also mentions the increased relationship between terrorism and organized crime and the need to boost collaboration between police forces, intelligence forces, border authorities and judges at the national level, and with foreign intelligence services at the international level in order to fight organized crime as well.[120]

The need to improve the information and intelligence systems ended in the creation of the CICO, Centro de Inteligencia contra el Crimen Organizado [Center for Intelligence against Organized Crime], composed of policemen, Guardia Civil, with the participation of policemen from autonomous communities, members of the Border Control Service and the collaboration of the Armed Forces, when needed. The Strategy called the authorities to strengthen the intelligence capacities and resources of the CICO and to improve coordination inside and outside the country with the police forces and intelligence services of different countries.[121]

---

[117] See Royal Decree 400/2012, of 17th February, from which the basic organic structure of the Home Department is developed [Real Decreto 400/2012, de 17 de febrero, por el que se desarrolla la estructura orgánica básica del Ministerio del Interior]. The CNCA depended previously on the Unified Command Executive Committee inside the Home Department (CEMU) [https://elpais.com/elpais/2004/05/28/actualidad/1085732229_850215.html]; The Royal Decree 991/2006 modifying the structure of the Home Department placed it under the oversight of the Secretary of State for the Home Department – Ministro del Interior [Real Decreto 991/2006, de 8 de septiembre, por el que se desarrolla la estructura orgánica básica del Ministerio del Interior]. Let us remember that the CNI is within the Defense Department.

[118] https://www.elmundo.es/elmundo/2007/01/18/espana/1169116906.html

[119] https://www.europapress.es/nacional/noticia-sistema-informatico-cnca-recogera-todas-investigaciones-curso-evitar-descoordinacion-cuerpos-20070118151009.html

[120] Estrategia de Seguridad Nacional (2011), p. 53.

[121] Estrategia de Seguridad Nacional (2011), p. 54.

In October 2014, the Government created the Center for Intelligence against Terrorism and Organized Crime (CITCO), merging the CNCA and the CICO.[122] The Government connected the need to merge both centers to the blurring of the line separating organized crime and terrorism. The Government explained that terrorist groups were increasingly using organized crime as a way of funding their activities, committing serious crimes such as drug trafficking, cybercrime, fraud and aggravated burglaries. It explained that in Spain, at least 20% of people imprisoned for allegedly belonging to jihadi terrorism between the years 2005 and 2011 had already been in prison for their participation in committing other crimes. The recruitment in prisons of common criminals to join the jihad, and the globalization that is so directly related to terrorism and organized crime, made necessary and urgent, in the opinion of the Government, a new methodology to confront those threats, which should pursue joint coordination and analysis efforts among agencies to face this new challenge.[123]

According to the law, this new Center would be the organ in charge of the reception, integration and analysis of the strategic information available in the fight against all types of organized crime, terrorism and violent radicalism, and of designing specific strategies against those threats, as well as, where appropriate, the establishment of criteria of action and operational coordination of the agencies acting in those fields in the case of concurrent investigations.[124] In particular, the CITCO would receive, integrate and analyze operational information and analysis related to organized or particularly serious crime, terrorism and violent radicalism that were relevant or necessary for the elaboration of strategic and prospective criminal intelligence in relation to these phenomena, integrating and channeling all of the operational information they receive or capture to the State police forces.[125] It would

---

[122] A new subdirectorate-general, under the oversight of the Undersecretary of State for Security [Secretario de Estado de Seguridad] in the Home Department. See http://www.interior.gob.es/prensa/noticias/-/asset_publisher/GHU8Ap6ztgsg/content/id/2624738 and Royal Decree 873/2014 [Real Decreto 873/2014, de 10 de octubre, por el que se modifica el Real Decreto 400/2012, de 17 de febrero, por el que se desarrolla la estructura orgánica básica del Ministerio del Interior].

[123] See http://www.interior.gob.es/prensa/noticias/-/asset_publisher/GHU8Ap6ztgsg/content/id/2624738

[124] Single Article s. 2 of the Royal Decree 873/2014 [Real Decreto 873/2014, de 10 de octubre, por el que se modifica el Real Decreto 400/2012, de 17 de febrero, por el que se desarrolla la estructura orgánica básica del Ministerio del Interior].

[125] As regards the incorporation of the autonomous police forces in the CITCO, this with the approval of the central Government prepared two identical protocols for both the Ertzaintza and the Mossos d'Esquadra. The Ertzaintza signed it at the Security Meeting of 14th June 2017. The Generalitat (Catalan government) signed the protocol with the Central Government on 10th July 2017. This protocol contained the conditions for the participation of the autonomous police forces in the CITCO. According to the Sixth point of the Protocol signed with the Generalitat, the two administrations undertook to support actions and coordinate themselves in operations that resulted from the collection of information, analysis, definition of strategies and execution of operations in the field of counter-terrorism. The

determine and establish, in cases of joint or concurrent intervention, the criteria for coordination and action of the operating units of the State police forces, and of those from other intervening agencies[126] The actual regulation of the CITCO can be found in Royal Decree 952/2018, of 27th July, which attributes to the CITCO more or less those same powers. It adds that the National Passenger Information Office (ONIP), which acts as a national Passenger Information Unit (PIU) provided for in European law, will be located at the CITCO; the Judicial Police Unit for terrorist Offenses (TEPOL) will also be sited at the CITCO, which will also develop the functions entrusted to the Main NATO-EU Subregister.[127]

5. The SCI-SICOA Database for the Fight against Terrorism and Organized Crime

The creation of the CITCO meant an intensification in the fight against terrorism. The number of investigations on terrorism increased by 62% in the first year, from 145 in 2014 to 236 in 2015. In 2016, 248 investigations were open, in total 802 were

---

ultimate goal was to improve the knowledge about terrorist networks, with Catalonia being a key territory. "Both bodies guarantee the timely exchange of information and intelligence of a strategic nature about organized crime, especially in cases of terrorism and radicalism."

The press gave notice that the Catalan autonomous police forces would meet with the CITCO every three months at the least. All this information came to light after terrorists attacked people at "Las Ramblas" in Barcelona, in the summer of 2017. The press explained that the Mossos had not finalized its incorporation into the CITCO because the Mossos had to adapt its computer systems to those of the CITCO (and there is a discussion whether there was any political will to do so or was just a technical question). The Ertzaintza did not have any difficulty in modifying their systems to join the anti-terrorists. The databases (CITCO and Mossos) are in different programs so the definitive dump could not be taken into effect until the Mossos made the necessary modifications in order to share its data. The press reported in 2015 that the incorporation of the Mossos in the CITCO would mean the access of the Mossos as a full-fledged member into the Investigations Coordination System (SCI-SICOA). [See the following press releases: https://www.libertaddigital.com/nacional/el-gobierno-compartira-informacion-antiterrorista-con-los-mossos-mientras-desmantela-el-mando-de-la-guardia-civil-1276288097/; https://www.elmundo.es/espana/2018/08/27/5b8304d546163fb71f8b45cf.html; https://gaceta.es/noticias/interior-incluira-mossos-ertzaintza-lucha-antiterrorista-28052015-2129/.]

[126] *Ibid*. According to this the CITCO will also prepare annual reports on the situation of organized crime, terrorism and violent radicalism in Spain, as well as a periodic evaluation of the threat in these fields. It will propose national strategies against organized crime, terrorism and violent radicalism and update them permanently, coordinating and verifying their development and execution, and it will develop the specific powers that the different provisions and agreements, both national and international, entrust to the Home Department in matters of fighting against terrorism and organized crime.

[127] S. 2.3 (c) Real Decreto 952/2018, de 27 de julio, por el que se desarrolla la estructura orgánica básica del Ministerio del Interior.

still alive that year.[128] Until July 2017, 127 new investigations were incorporated into the databases of the CITCO, and 814 continued as active investigation lines.[129] Regarding organized crime, the databases incorporated 4,159 new investigations from January to May 2017.[130]

The increase in the incorporation of data into the SICOA improves the coordination between the different police and intelligence forces and provides the ability to rapidly detect matches in some of the elements of different investigations (people, establishments, accounts, etc.).[131]

There is a Coordination Area at the CITCO whose mission is to detect matches in the data on physical or legal persons, telephones, homes, web pages or vehicles involved in investigations.[132] Powerful databases make it possible to track coincidences beyond counter-terrorism investigations, merging data to detect links to ongoing investigations of organized crime or drug trafficking.[133] According to the press gathering the information from a source aware of the operation of the system, apparently the SICOA is not a database where you put the name of a jihadist and all of his or her data appears. The system works as a "blind file" in which the competent bodies must include relevant aspects of their ongoing investigation, such as a name, a license plate, or an email address, and when another police force is on the track of the same people, SICOA alerts and police forces have an obligation to coordinate themselves and to decide who is responsible for the investigations. Sometimes they

---

128 https://www.elespanol.com/espana/20170702/228227307_0.html; https://elpais.com/politica/2016/08/18/actualidad/1471510282_948539.html

129 https://www.elespanol.com/espana/20170702/228227307_0.html

130 https://www.elespanol.com/espana/20170702/228227307_0.html

131 https://elpais.com/politica/2016/08/18/actualidad/1471510282_948539.html. Likewise, there is permanent contact with the Public Prosecutor's Office in order to avoid duplication of actions in different courts. The CITCO, in coordination with the Public Prosecutor's Office, detects the different dysfunctions or duplicate data which, by different circumstances, have not been included in the coordination system and which could affect different central courts of Instruction.

Since the creation of the CITCO there has been a significant increase in coordinated operations: up to 173 cases in 2015, 28% more than those registered in 2014 (that is, 135) when the CITCO was not in operation. From 2012 until August 2016 there had been 703 coordinated operations [https://elpais.com/politica/2016/08/18/actualidad/1471510282_948539.html].

In 2016, the CITCO acted as arbitrator in five meetings in the face of the specific discrepancies between the police bodies responsible for anti-terrorist investigations. From January until May 2017, the police forces developed jointly 310 investigations (14%). On eleven occasions, the CITCO had to issue coordination agreements in the absence of an initial consensus, although in half of them the operations were completed in a joint manner [https://www.elespanol.com/espana/20170702/228227307_0.html].

132 https://www.elespanol.com/espana/20170702/228227307_0.html. Until August 2016, CITCO had detected more than 300 matching data. [https://elpais.com/politica/2016/08/18/actualidad/1471510282_948539.html].

133 https://www.elespanol.com/espana/20170702/228227307_0.html

decide to create joint groups that have reported successful police operations. There is a complex coordination manual that fixes the criteria and the way in which the data should be recorded.[134]

In March 2017, the Government was questioned by a socialist member of Parliament about the CITCO and whether a new database for special cases had been created. The Government denied the creation of this new database and explained that there were only two different data systems at the CITCO: The Coordination of counter-terrorism Operations' System (SICOA), and the Investigations Coordination System (SCI, the old SRI).[135] According to the Government, access to the Investigations Coordination System is limited to three analysts, members of the State Security Forces, and access to the Anti-Terrorist Investigations Coordination System is restricted to only two analysts. Neither members of the manager team of the CITCO nor the Director of the Center are authorized to access the systems.[136]

The Order INT/1202/2011, of 4th May on the personal data files of the Ministry of the Interior regulates the SCI computerized database. The Order says that the Investigations Registration System (SRI, now SCI) manages and detects the matches of objective data of all police investigations; there is the Coordinated Operations Database to complement it, for the integral management of the matches found. The data included in the databases are: [137]

1. Investigation (operation name, origin reference number and reference number in the SRI)
2. Natural Persons (name and surname, DNI/NIE/Passport)
3. Legal Persons (denomination and NIF)
4. Telephones
5. Real Estate (location: Town, street, number)
6. Means of transport (vehicles, ships, aircraft; license plate, name of means of transport)
7. Bank Accounts Used (account number)
8. Web Pages used for criminal offense (denomination of the page in Internet)

---

[134] https://www.elespanol.com/espana/20170820/240476498_0.html

[135] The SRI was created according to Instruction 5, of March 21, 2005, of the Secretary of State for Security and supplemented with the instructions 12/2005, of 8th July, and 1/2007, 12th January.

[136] Question: "Apertura de un fichero restringido de casos "especiales" por el Centro de Inteligencia contra el Terrorismo y Crimen Organizado (CITCO). (184/005111)" [Opening of a restricted database for special cases by the CITCO]. BOCG [Parliament, Lower House Official Journal]. Congreso de los Diputados Núm. D-71 de 19/12/2016. See the answer in Spanish in the web page of the Congreso de lo Diputados.

[137] See Annex I. Undersecretary of Security. 5th Database: Operations Coordination, Order INT71202/2011, of 4th May.

9. Email Addresses (full Internet address)
10. Investigating unit and police officer (Body, Unit and Group that develops the investigation. Name and surname, Body, job, position, contact telephones and email address of the operative responsible for the investigation)
11. Substances intervened or investigated (drug type and apprehended quantity)
12. Geographical Location (places or locations where it was intervened)
13. Types and subtypes of crimes investigated (generic and specific to each offense in accordance with the Penal Code)
14. Organized crime Indicators (number of detainees)
15. Denomination of the criminal organization (name of the transaction)
16. Effects intervened or investigated (quantity of real estate, number and description of computer or audio-visual means, quantity and denomination of chemical products, etc.)
17. Other intervened goods
18. Relationships between people investigated

According to the Royal Decree, the data can be transmitted to other police forces (in particular to those of autonomous communities) and to the Courts and the Public Prosecutor[138] and to international organizations and foreign countries in application of treaties or agreements to which Spain is a party.

On the other hand, anti-terrorist and organized crime investigations, and therefore their data, are declared secret.[139] Therefore, all data introduced into the system by the police forces and other bodies of the State and by the Deputy Directorate of Border Surveillance are declared secret.[140]

---

[138] The Order justifies it under the provisions of articles 3 and 45 of Organic Law 2/1986 of 13th March, which regulates the Security Forces and article 11.2 d) of Organic Law 15/1999 of 13th December (now derogated by Organic Law 3/2018, of 5th December on data protection and guarantee of digital rights).

[139] Agreement of the Council of Ministers of 16th February 1996, classifying certain matters (under s. 4 Official Secrets Acts), classifies the structure, organization, means and operational techniques used in the fight against terrorism by the Forces and Security Bodies of the State, as well as their sources and the information or data that can reveal them as secret, and also those Antiterrorist Databases of the Penitentiary Administration. On the other hand, the Agreement of the Council of Ministers (Government) of 6th June 2014 declares secret the structure, organization, means and operative techniques used in the fight against organized crime by the Security Bodies of the State, as well as their sources and as much information or data as may be revealed. The Official Secrets Act is Act 9/1968, of 5th April, modified by Act 48/1978, of 7th October.

[140] Answer by the Government in http://www.congreso.es/l12p/e2/e_0026544_n_000.pdf

6. Information and Data Sharing between Police Forces and Intelligence Services

There is a small part of the work of the CNI – around 10% according to the Director of the CNI – which is common with that of the police forces.[141] The natural inclination of police forces and the CNI would be to share data on those common fields, but obviously this would affect the right to data protection included in article 18.4 SC, and, therefore, it cannot be done without respecting the requirement to limit fundamental rights.

The law on data protection in Spain has changed recently due to the necessity to adapt to the new Regulation (EU) 2016/679.[142] In December 2018, the Spanish Parliament passed Organic Law 3/2018, of 5th December, on the Protection of Personal Data and the guarantee of digital rights. This law substituted Organic Law 15/1999, of 13th December, on the Protection of Personal Data. Directive (EU) 2016/680 of the European Parliament and of the Council of 27th April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, has not been implemented yet in Spain. Because of this, the police forces' databases are still regulated by Organic Law 15/1999.[143]

Organic Law 15/1999 excludes from the applicability of the law those data files subject to the Official Secrets Act (s. 2.2 (b)), and those data files created for the investigation of terrorism and other serious organized crimes (s. 2.2 (c)).[144] S. 2.2 (c) states that nonetheless, the person in charge of the file has to communicate this fact to the Data Protection Authority (s. 2.2 (b) and (c) Organic Law 15/1999). Regarding all other cases, the law states that the police forces can process personal data without the consent of the person affected if there is a real danger for public security or in

---

[141] The CNI Director said its mission was to guarantee the security of the population in a broad sense, and pointed to protecting against terrorism, avoiding cyberattacks, looking after Spanish companies able to operate in foreign countries, knowing the migrant flows or guaranteeing that the gas pipes that bring gas to our country are not cut on its way through countries in conflict. The CNI said this in an act in Valencia [see https://www.levante-emv.com/comunitat-valenciana/2018/03/02/director-cni-servicio-secreto-mejor/1686449.html].

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

[143] See Transitory Clause number 4 of Organic Law 3/2018.

[144] See footnote 91 *supra.*

order to repress criminal acts (s. 23 Organic Law 15/1999).[145] The Data Protection Act forbids the use of the data for different purposes incompatible with those that were the ones alleged for gathering the data (s. 4. 2 Organic Law 15/1999). The files must differentiate between categories of data in relation to the reliability of such data (s. 23 Organic Law 15/1999).

The data cannot be transmitted to other administrations without the consent of the affected person, except if there is a law authorizing it [the Constitution reserves the regulation of fundamental rights in articles 53.1 and 81 to a law]. There cannot be indiscriminate transmission of data among public administrations, as the data are specific to the purpose that determined their gathering. The transmission of data among administrations can only be carried out if the Data Protection Act authorizes it or if there is an express law authorizing it.[146] This law can authorize the transmission of the data if the goal is to protect other constitutional rights or public constitutional interests observing the principle of proportionality.

The Data Protection Act contains a provision that seems to permit public administrations to transmit data to other administrations as far as it is not for the exercise of different powers or as regards different subjects (s. 21 (1) Organic Law 15/1999). Royal Decree 1720/2007 seems to confirm this point: the transmission of data amongst administrations can be done if it pursues the exercise of identical powers or concerns the same subject matter (s. 4 (c) of Royal Decree 1720/2007, of 21st December). The Constitutional Court has stated in any case that the transmission of data for purposes different to those that legitimized its collection amounts to new data processing and would require the consent of the affected person (STC 292/2000, of 30th November, §13[147]).

Order INT/1202/2011, which is not a law, regulates the coordination of the operations database regarding organized crime (SCI). According to the INT/1202/2011 order, the SRI (now SCI) database is created to manage, monitor and control organized crime operations, coordinated or in coordination phase, as well as the results thereof. The data on the database are provided by the state police forces and other services or institutions (which include the CNI) in relation to their respective investigations on criminal groups dedicated to drug trafficking and organized crime (there is no definition of the time period in which the data can be kept in that database!). The creation of the database pursues the coordination between the different police forces of the state and other services or institutions, based on their powers to investigate drug trafficking and other forms of organized crime, as well as the coordination

---

145 On the provisions regulating the police forces databases in the Data Protection Act see: *Tejerina Rodríguez, Ofelia*: Seguridad del Estado, p. 164 ff.

146 STC 17/2013, of 31st January, § 4.

147 The judgment 292/2000, of 30th November is a key judgment as regards the right to data protection in Spain.

with other international centers with the same competencies and the statistical management of the aforementioned operations.

From the regulation of the SCI and various press releases it seems that police forces and the CNI incorporate the data of their investigations into the database in order to coordinate their operations (those data are accessed by two or three analysts, as we saw, depending on the issue, whether it concerns organized crime or terrorism). The problem is that no law regulates this database. The police forces and the CNI do not gather data for the same purpose. The police forces gather data for law enforcement purposes, in order to investigate crime under the orders of the public prosecutor or judges, and subject to particular rules as regards the collection of evidence. The CNI collects data for the prevention of threats and dangers to national security, subject to a different threshold regarding the collection of information; even if the law includes amongst the threats that the CNI has to help prevent terrorism and organized crime, it exercises this function with a different focus, its main aim being to provide the Prime Minister and the Government with intelligence (Art. 1 CNI Act).[148] If the CNI were to share data with the police, who work with different parameters and higher thresholds, there should be a specific law allowing it, and actually there is no such law in Spain. This SCI-SICOA database does not fulfill the constitutional requirements.[149] There could probably be circumstances in which both the CNI and the police forces would be legitimized to share data, but those circumstances should be delineated by law and be those necessary in a democratic society to protect national security. The law should determine who could access the database and the time period in which the data could be kept in that database.[150]

Article 5 CNI Act declares secret all databases of the CNI, and s. 2.2 (c) Organic Law 15/1999 states that this law is not applicable to all databases created for the investigation of terrorism and other serious organized crimes (though the existence of such a database has to be communicated to the Data Protection Commissioner, indicating the general characteristics of the database and its purpose).[151] Because of this special regime, we have no knowledge of the functioning of the SICOA database.

---

[148] A different problem is the secrecy of the sources and methods of the intelligence services. It is possible that in many occasions the intelligence services won't share information in order not to damage those sources and methods.

[149] The SCI-SICOA allows that the data also be transferred to other police forces (those of the autonomous communities) and to the prosecutor and judges. The law refers to articles 3 and 45 of Organic Law 2/1986, of 13th March. Those provisions refer just to the principle of cooperation, and they would not suffice by themselves to serve as a basis for the transmission of data (though in this case we can accept that those police forces have all the same functions, and the reference to Organic Law 15/1999 will suffice). Article 11.1 (d) allows this transmission to the public prosecutor and the judges for the exercise of their functions.

[150] S. 22 (4) of the Data Protection Act 15/1999 states that personal data recorded for police purposes will be cancelled when it is no longer necessary for the inquiries that prompted their storage.

[151] See footnote 91 *supra.*

Public security and national security are legitimate grounds to limit the right to data protection, but the existence of secret databases to coordinate antiterrorist operations amounts to such serious interference with the right to data protection that the law should establish mechanisms in order to protect citizens against abuses. The only guarantee that the Spanish law offers to citizens in the field of terrorism and organized crime is the duty to inform the data protection authority about the existence of the secret database, its general characteristics and purpose (s. 2.2 (c) Organic Law 15/1999), but the Data Protection Commissioner has no effective powers to remedy any violation in these particular cases. In the case of those databases classified as secret, the only possible remedy against violations of the right to data protection could come from the Parliamentary Commission in charge of overseeing the CNI, which is the only one with access to those databases. This situation does not really provide citizens with effective remedies in my opinion.[152]

7. Use of Intelligence Information in Court

7.1 Classified Information and Criminal Procedure in Spain

According to articles 2 and 4 of the Spanish Official Secrets Act of 1968, reformed in 1978, the acts, issues, documents, data or objects which when obtained by non-authorized people could threaten or damage national security can be classified by the Executive as secret. The law can also classify any information as secret (s. 1.2 Official Secrets Act).

The CNI Act establishes that the activities of the National Intelligence Center, as well as its organization and internal structure, means and procedures, personnel, facilities, databases and data centers, sources of information and information or data that may lead to the knowledge of the foregoing matters, are classified with the degree of secrecy in accordance with the provisions of the Official Secrets Act. The Official Secrets Act provides that classified information cannot be communicated, disseminated, published or used outside the limits established by the Act (s. 13 Official Secrets Act). The Act contemplates that the Lower House (*Congreso*) and the Upper House (*Senado*) will have access to classified information (s. 10.2 Official Secrets Act), but the CNI Act has exempted from this knowledge information coming from foreign intelligence services or international organizations that will be ruled by the agreements and treaties signed on the matter.

---

[152] See s. 11 CNI Act. About the Parliamentary Committee that oversees all secret information see *Sánchez Ferro, Susana*: Parliamentary and specialized oversight of security and intelligence agencies in Spain (2011), in Parliamentary and Security Oversight of Security and Intelligence Agencies in the European Union, Directorate General for Internal Policies, Policy Department c: citizens' rights and constitutional affairs, European Parliament, Annex A, pp. 266–276.

The law does not say anything about allowing judges access to classified information. In the Act, the prevalence of national security over the judiciary seems to be absolute. Article 417.2 CCP provides in section two that civil servants (also from the military) cannot be obligated to act as a witness if they cannot do so without violating their oath to secrecy because of their position or when their superior does not allow it. Nonetheless, in 1997 the Supreme Court, in the "Cesid documents case" (*caso de los papeles del Cesid*),[153] opened a window as to the possibility of incorporating that information in a criminal procedure.

The "Cesid documents case" originated when famous Judge Garzón, at the time enquiring Judge of the Audiencia Nacional (the Court that decides on terrorism cases), was investigating the killing of some people presumably linked with ETA (the terrorist group). There were suspicions that those in charge of the fight against ETA, including the intelligence services, had executed and planned the killings of two members of ETA. Judge Garzón asked the CESID to inform him about the existence or nonexistence of a group called GAL (Grupos Armados de Liberación: Liberation Armed Group) who would have been those responsible for the killing of those supposed members of ETA. Garzón also asked for documents that would prove the participation of members of the police forces or the CESID in those criminal activities.[154] The Director of the CESID answered Judge Garzón that he could not fulfill his requirements because the information was covered by the state secrets privilege according to the Official Secrets Act of 1968.

Other petitions by Garzón followed, one asking the Director of the CESID (there was still no CNI) to testify. The Director appeared before the Court to testify but he did not reveal the secret information. Moreover, the Government, by Agreement of the Council of Ministers of 2nd August 1996, denied the declassification of the documents, saying they were covered by the state secrets privilege. The plaintiffs in the judicial proceedings appealed the Government's decision to invoke the state secrets privilege to the Supreme Court.

The Supreme Court, in the "CESID documents case" – judgment of the Supreme Court of 4th April 1997[155] – declared that the classification of information by the Government was a political act related to the most sensitive spheres of power, linked with the survival of the constitutional order – defined as a complex of political and legal values that have to be protected against those who want to attack them by violent means and through attacks to the external and internal security. The Court

---

[153] *Vid.* Supreme Court judgment of 4th April 1997 (STS 4 abril de 1997), Appeal n. 726/1996. There are other judgments of the Supreme Court of that same date related to the same case and declaring exactly the same so we use this case as a model.

[154] The documents consisted of some 'office' notes, a document about illegal armament and a report about activities carried out by members of the security forces in the fight against terrorism in the south of France.

[155] Appeal n. 726/1996.

declared that the documents requested by Garzón affected the national security of the country, as part of a set of studies, measures, information, decisions and actions directed to fight terrorism, because terrorism wants to alter the constitutional order, using as one of its methods violence against life and physical integrity. But despite all this, the Supreme Court ruled that it was competent to review the Government's decision on the merits and decide whether those documents should be secret according to the law, as the law had defined through attainable concepts the limits or previous requirements to which these acts of political direction were subject (the information should threaten or damage national security).

According to the Supreme Court, articles 9.1 and 24.1 SC obliged the Court to review the possible abuses or failures to comply with the law by the Government, when taking the decision to classify the information.[156] The Court asserted that it could control the concurrence of elements that either suppressed the effects on national security of the documents or reduced them – balancing the interests at stake – giving then preference to the due process clause and the rights invoked by the appellants, mostly those contained in article 24 SC, which deals with the right to a public trial without undue delays and with full guarantees and the right to use relevant evidence (notice here that the evidence was requested by the prosecution, not the defense).[157] The Spanish Supreme Court considered itself legitimate to control the documents *in camera*, without the presence of the prosecution and the defence (parts of the process *a quo*), even when there was no similar procedure regulated in our legal system at the time. The Court applied a balancing test to the case, analyzing document by document to decide when national security had to give way to the right to the relevant evidence because of the special importance of that evidence in the case. The Court decided the value of each document to the due process, weighed them in relation to the harm that their disclosure could do to national security, and thus decided which document would have to be declassified by the Government and disclosed to the judge and the parties to the proceedings. The Government then proceeded to declassify the documents according to Court order [the Official Secrets Act (s. 7 Official Secrets Act) gives the power to declassify those documents to the Government and not to the judges]. With this solution the parties' right to a public

---

156 Article 9.1 SC: The citizens and public powers are subject to the Constitution and the legal order. Article 24.1 SC: All persons have the right to the effective protection of the judges and courts in the exercise of their rights and legitimate interest.

157 Article 24 SC:

1. Every person has the right to obtain the effective protection of the judges and the courts in the exercise of his or her legitimate rights and interests, and in no case may he go undefended.

2. Likewise, all persons have the right of access to the ordinary judge predetermined by law; to the defense and assistance of a lawyer; to be informed of the charges brought against them; to a public trial without undue delays and with full guarantees; to the use of evidence appropriate to their defense; to not make self-incriminating statements; to not declare themselves guilty; and to be presumed innocent.

and adversarial trial would be respected, as the material would be incorporated into the case once it had been declassified by the Government 'by order of the Supreme Court'.

In conclusion, in order to incorporate any piece of secret evidence to a criminal trial, it must first be declassified by the Government, though the decision of the Government not to declassify the documents can be controlled by the Supreme Court (Administrative branch), which can order the Government to execute the declassification in particular instances, as we have seen.

7.2 Criminal Procedure and Formal Reports (*denuncias*) by the CNI

As Lorena Bachmaier and Antonio del Moral García explain in their book *Criminal Law in Spain*, normally the police "are the first to receive the *notitia criminis* (…). Once an offense has been reported, there are a myriad of possible activities to perform depending on the type of offense. If it is certain that a crime has been committed, the police will gather all the information concerning the criminal fact: collect elements or pieces of evidence, take photographs, interrogate, and collect information of witnesses and of the victim; request the presence of a physician if there are injured persons; arrest the suspect, if he can be found; and interrogate him. […] The activities that have been performed and their results will be detailed in a written report (so-called *atestado*). After that, within a maximum time of twenty-four hours the police must hand the report (*denuncia*), together with their own investigative record (*atestado*), either to the public prosecutor or to the investigative judge. Most often they pass it on to the judge. [One of the reasons is] that the investigating judge accords the power to authorize investigative measures that restrict fundamental rights (…)".[158] As we have already seen, the conditions in which a judge in a criminal procedure can allow the police to adopt those measures have a different threshold in order not to violate fundamental rights.

But, what if the intelligence service is the one to report the crime to the public prosecutor or the judge and the information may have been obtained using intrusive techniques affecting fundamental rights?

Among Spanish scholars there was a discussion about the constitutionality of the CNI Judicial Control Act of 2002 between those who thought the Act was unconstitutional, because the only legitimate ground to intercept communications or search the dwelling should be in the context of criminal proceedings respecting all the exigencies and thresholds established by the jurisprudence of the Constitutional Court

---

158 *Bachmaier, Lorena & Del Moral García, Antonio*: Criminal Law in Spain, p. 207.

regarding those kinds of interceptions,[159] and those who agreed that the Act was constitutional.[160] Those in favor of the constitutionality of the CNI Judicial Control Act argued that the aims of the police interception and those of the CNI interceptions were different and therefore there was no problem of constitutionality of the law: the police intercept communications or enter a home in order to seek evidence of the commission of a crime and to incorporate that evidence into a criminal proceeding; they pursue the repression of crime; therefore, they must respect the thresholds and guarantees established by the Constitutional Court, seen *supra*; but interception of communications or home searches made by the intelligence services do not have that aim – they are not directed to destroy the presumption of innocence in the criminal process – but seeks to gather information in order to prevent risks and dangers to national security. The aim of the intelligence services is just to analyze the information and pass it on to the competent political organs of the State.[161] Therefore, the interception of communications by the intelligence services, according to those authors, has a different threshold and should comply only with the necessary guarantees in order to limit the right to privacy (quality of the law test, proportionality test…), but not with those guarantees linked to article 24 (2) SC, which regulates the right to due process, given that the aim of interceptions by the intelligence services is not obtaining evidence.[162]

---

[159] See *Gimbernat Ordeig*: "La vida de nosotros".

[160] *González Cussac*, *J.L.*: Intromisión en la intimidad. The jurisprudence of the Constitutional Court requiring circumstantial evidence to legitimize the interception of communications and an objective base to do so, linked to the interception of communications in criminal contexts, would not apply to the interception of communications carried out by the intelligence services, according to this theory, though the authors who defend it do not clarify which would then be the threshold, if any, to intercept communications for national security purposes [see *Pérez Villalobos, Mª Concepción*: Derechos fundamentales, p. 82. *González Cussac, J.L.*: Intromisión en la intimidad, p. 90]. The CNI Judicial Control Act says that the Court will authorize the measures affecting the secrecy of communications or the inviolability of the home when they are necessary to fulfill the functions of the Center (Single Article (1) of the CNI Judicial Control Act). The Director of the CNI has explained that, in practice, the Judge of the Supreme Court "has access to the Intelligence Directive, which is secret, in order to be able to confirm that it is in the Intelligence Directive – the National Security goal, we guess – and authorise the interception or search if the intrusion in the rights of the people is necessary to guarantee the security of the Spaniards" [https://www.levante-emv.com/comunitat-valenciana/2018/03/02/director-cni-servicio-secreto-mejor/1686449.html]. If the law does not include any particular threshold, that could mean an open door to prospective investigations and would put in danger the principle of proportionality.

[161] *González Cussac, J.L.*: Intromisión en la intimidad, p. 88.

[162] *González Cussac, J.L.*: idem, p. 90. When the intelligence services intercept communications, they do not have an obligation to notify the affected person, according to the Spanish legislation, the Public Prosecutor does not intervene in those procedures, and it is the Undersecretary of State who destroys the data and not the judge. On the other hand, as regards home searches, in the CNI Judicial Control Act there is no regulation as to the notification to the affected person of the results of the intervention when it has ceased or there is no more danger to national security, or as to the necessary presence of the secretary of the judge in the searches, contrary to what happens in the regulation of home searches in the

Problems arise when the intelligence services report to the public prosecutor or to the court the commission of a crime. The Supreme Court had to address this very interesting question in its judgment of 6th December 2010.[163] This judgment was given in a very particular context, and therefore the decision of the Supreme Court might in a way have been influenced by it. The case concerned a man accused of having committed treason. The man worked for the CNI; at work he had accessed some documents classified as secret according to the Official Secrets Act of 1968 without proper authorization. He took the secret documents out of the Center, kept them in different devices and documents and wrote some letters to the counselor of the Russian Embassy in Madrid offering the Russians his collaboration. He offered to keep them informed about who was who at the CNI, of the methods used by the CNI against Russia, the structure of the CNI, missions, targets and aims of the technical division, political interests of Spain in its foreign policy, etc.[164] After a "security investigation" inside the CNI, the Director of the CNI reported the case to the public prosecutor.[165]

In the formal report (*denuncia*) to the public prosecutor, the Director of the CNI assured that the aforementioned documents were in the house of the former CNI member and explained how this former CNI member had a suspiciously high economic status, which did not match the one he would have just according to his work at the CNI. The public prosecutor did not have access to the "security investigation" carried out by the CNI. In any case, he came to the conclusion that the facts reported constituted a crime and handed the case over to the investigating judge. The investigating judge authorized the entry and search of the home of this man, now with all the guarantees of the Code of Criminal Procedure but through a very "laconic" resolution, as he did not have much data about the said unlawful conduct apart from the information received from the CNI. The man was found guilty and sentenced to 12 years in prison by the Audiencia Provincial for committing a crime of treason (Provincial Audience, a court of law).

---

criminal context, regulated by the CCP. On the other hand, as *Pérez Villalobos and González Cussac* remark, there is a lack of regulation in the CNI Judicial Control Act as regards tracing people, crossing informatics data, and installing microphones or cameras in offices, homes or vehicles [*Pérez Villalobos, Mª. Concepción*: Derechos fundamentals, p. 95 and *González Cussac*, *J.L.*: Intromisión en la intimidad, p. 95] nor does the CNI Judicial Control Act regulate the remote search of computers, or the recording of conversations in open spaces, contrary to what the CCP does.

163 Supreme Court Judgment, 2nd Chamber (Criminal branch), of 10th December 2010 [STS 7056/2010 - ECLI: ES:TS:2010:7056].

164 Supreme Court Judgment of 6th December 2010, §1 (Facts).

165 The public prosecutor is the one that charges a subject with a criminal offense, whenever a crime has been committed, and presents the case before the court. In Spain the police have no prosecution functions; it is the public prosecution service that is responsible for the prosecution of all criminal offenses [*Bachmaier, Lorena and Del Moral García, Antonio*: Criminal Law in Spain, p. 30].

The man's defense counsel appealed to the Supreme Court, alleging that there had been a violation of article 24.2 SC[166] because the oral trial at the Audiencia Provincial had been closed to the public and the media (the defense considered this to violate the right to a public trial with all the guarantees) and considered also that there had been a violation of his right to use all means of evidence relevant for the defense (in relation to the right to the secrecy of communications and the inviolability of the home, and the right to be presumed innocent). The accused complained of the lack of transparency and the impossibility of knowing the scope and extension of the security investigation carried out by the CNI, which was at the origin of the criminal procedure.

The court analyzed the question of the right to a public process and reminded the accused that this right is not an absolute right. Article 120 (1) SC establishes that judicial proceedings shall be public, with the exception of those provided for in the laws of procedure. The court also added that some articles of the CCP allow for the closure of the procedure; particularly article 232 of the Judicial Power Organic Law (Ley Orgánica del Poder Judicial – LOPJ): The judge can limit the publicity of the proceedings and declare the secrecy of all or part of the procedure, exceptionally, for reasons of public order and the protection of other rights and freedoms. The Audiencia Provincial decided to close the trial because there were many agents of the CNI intervening in the procedure and a relevant number of documents linked to the activities of the CNI that would be the object of questioning during the trial. The court concluded that there was no violation of the principle of publicity of the trial as the Audiencia Provincial had correctly balanced the rights and interests in play.

The Supreme Court then looked at the allegation of violation of article 24 (2) SC regarding the right to use means of evidence at the trial. The defense asked the court (Audiencia Nacional) during the evidence phase to ask the Supreme Court (Art. 127 LOPJ) to inform the defendant whether the former CNI member now being judged

---

[166] Article 24 SC:

1. Every person has the right to obtain the effective protection of the judges and the courts in the exercise of his or her legitimate rights and interests, and in no case may he go undefended.

2. Likewise, all persons have the right of access to the ordinary judge predetermined by law; to the defense and assistance of a lawyer; to be informed of the charges brought against them; to a public trial without undue delays and with full guarantees; to the use of evidence appropriate to their defense; to not make self-incriminating statements; to not declare themselves guilty; and to be presumed innocent.

The law shall determine the cases in which, for reasons of family relationship or professional secrecy, it shall not be compulsory to make statements regarding alleged criminal offenses. [For a full translation of the Spanish Constitution see https://www.boe.es/legislacion/documentos/ConstitucionINGLES.pdf.]

had been the object of any judicial investigation diligence (obviously he referred to those supposedly carried out by the CNI) before the case reached the public prosecutor and to receive full testimony of that if it had been the case. The end of this request was to clarify if there had been a violation of the defendant's fundamental rights preceding the formal report (*denuncia*), as the ex-member of the CNI had not known of its existence or scope.

The Audiencia Provincial sent the question to the Supreme Court, which declined to answer this petition, alleging that the activities of the Supreme Court judge in charge of the judicial authorization of the CNI activities are secret according to the law (Single Article (3) of the CNI Judicial Control Act). The testimony of the Director of the CNI did not clarify anything either; he made use of his right not to testify on questions that may affect the secrecy of methods of the CNI and questions that could affect national security. When he was asked about those "security investigations" he declined to clarify whether those investigations were still pending or whether he had applied for any authorization to intercept the communications or search the home of the former CNI agent to the Supreme Court.

For the defense, the determination of whether those searches and interceptions had existed was relevant. The accused alleged that the CNI Judicial Control Act was unconstitutional as it enabled prospective invasions of privacy and argued that if the "security investigation" was taken to court, it should be made public, since the accused and the public prosecutor did not have access to the measure as it took place.

The Supreme Court, recognizing that the nature of those acts adopted by the judge in charge of the control of the CNI activities was problematic,[167] concluded that there was no violation of article 24 (2) SC. It argued that, beyond the possible imperfections of the control system established by the CNI Judicial Control Act, the key question in order to evaluate the significance of the whole issue is that the judge who authorizes the CNI wire-tapping or the entry and search of the home is not acting as a jurisdictional body when he issues a warrant allowing those measures by the CNI, but that he is overseeing the intelligence service. The aim of the warrant is not the investigation of a criminal act, and the judge is just the person in charge of overseeing the intelligence service (Parliament decided so when it opted for such a control system). As the warrant is not issued in the context of any criminal procedure, it is not subject to the principles of contradiction and defense.

On the other hand, the Supreme Court understood that there is no continuity between the "investigation" done by the CNI and the criminal procedure (and referred again to the functions of the CNI, which are not oriented to clear up crimes) and

---

[167] The Court referred to the absence of any possibility to appeal the resolution of the judge who authorizes the measure, and the lack of judicial oversight of the measure once the judge has approved it [see §a of the Sentence of the Supreme Court].

rejected the argument that the "security investigation" carried out by the CNI had any role in the said criminal procedure. The CNI judge was not, according to the Supreme Court, an assistant to the investigating judge in the criminal procedure. The acts of the CNI are not evidence, according to the Supreme Court, and are not even part of the judicial proceedings; the judicial inquest and the CNI inquiries do not share the same principles or content and the fundamental rights in both acts are sacrificed for different reasons. In conclusion, for the Supreme Court the existence of a subsequent Criminal Procedure where the *notitia criminis* is linked with the "security investigation" or security file does not transform this file into a procedural act.[168]

The accused complained about the lack of knowledge of the scope and extension of the security investigation carried out by the CNI. The Supreme Court argued that the judge of the Audiencia Provincial had not considered it necessary to ask for the declassification of that particular file to the Government because he thought it was not relevant to the case. The Supreme Court understood that the resolution of the judge was correct as the accusation of treason was founded on solid evidence produced inside the criminal procedure, so that the discovery of the security file would have no impact on the result of the proceedings, and affirmed that if the security file existed, it would have been authorized by the Supreme Court judge in charge of the CNI (as if this was a definitive argument to make up for any possible imperfection of the whole procedure).[169]

Finally, the accused complained about the constitutionality of the second judicial warrant, the one given by the investigating judge of the Audiencia Provincial in the Criminal Procedure authorizing the entry and search of the former CNI member's home. He said the judge had ordered this measure just basing its decision on the "security investigation" carried out by the CNI, which he, the accused, did not know (as it was secret). The Supreme Court answered that the objective data obtained through this security investigation could suffice to order the said measure (although it agreed that the resolution of the judge ordering the measure was "laconic"). Those objective data existed; they were put at the disposal of the public prosecutor by the CNI in a public report that was handed to the judge with the formal report by the public prosecutor. The public prosecutor made them their own in the formal report (*denuncia*) that served as justification for the warrant.[170]

The Supreme Court concluded its reasoning by affirming that the CNI did not act in this case as uncontrollable judicial police. It had complied with its functions, trying to neutralize the flight of information towards foreign intelligence services. This

---

[168] See §2 (A) Supreme Court Judgment, 2nd Chamber (Criminal branch), of 10th December 2010.

[169] See §2 (C) Supreme Court Judgment, 2nd Chamber (Criminal branch), of 10th December 2010.

[170] See §4 (A) Supreme Court Judgment, 2nd Chamber (Criminal branch), of 10th December 2010.

was the cause of the security investigation, and this investigation, according to the Court, reached the point it could reach and was then transferred to the courts.

7.3 Additional Considerations on Criminal Procedure and the Intelligence Service

The Spanish Supreme Court has solved some of the issues regarding the incorporation of classified documents coming from the intelligence service into the criminal procedure or the possibility of commencing a criminal procedure when the *notitia criminis* comes from the intelligence services, but in Spain we still do not have systematic legal regulation of all the issues that can affect the criminal procedure when the intelligence services investigate criminal matters such as terrorism or organized crimes.

Firstly, as *Lorena Bachmaier* has pointed out, regulating the rules for the incorporation of classified information into the criminal procedure does not solve all the questions that arise in connection with the due process clause.[171] One key issue is whether information or intelligence gathered by the intelligence services can be admissible as evidence in the criminal procedure.[172] Contrary to the police forces, which cannot carry out purely prospective research based on the generic need to prevent or discover crimes or try to confirm their suspicions when they do not have more than that, mere suspicions, the CNI does not have to comply with the same standards and thresholds regarding its security investigations; it is subject to different and in some cases lower thresholds than the police forces, because its functions are configured as preventive in nature and that information is not regarded to be incorporated as evidence against the accused in the criminal procedure.[173] Moreover, there is the problem of the reliability of sources. This question cannot be excluded from the discussion of the parts in the procedure.[174]

Secondly, there is no legal regulation of the obligations that arise from the discovery of a crime by the intelligence services like ones that exist in other countries such

---

[171] *Bachmaier Winter, Lorena*: Información de inteligencia, p. 97.

[172] Intelligence reports made by the police forces has been admitted as evidence in the criminal procedure. There was a discussion on the nature of that type of evidence [see *Bachmaier Winter*, *Lorena*: Información de Inteligencia, pp. 69–87; *Gudín Rodríguez-Magariños, Faustino*: La presunta prueba pericial; *Castillejo Manzanares, Raquel*: La prueba pericial]. See STS 65/2019, of 7th February, which considers this type of evidence as expert evidence (and in the case witness evidence) or STS 104/2019, of 27th February, which considers it expert evidence (and in the case also documental evidence).

[173] *Ibid*, *pp.* 94 and 97–98. In the CESID documents case, the documents were used against the intelligence services men that committed the killings; they were not documents investigating third persons appertaining to terrorist networks or organized crime.

[174] *De Llera Suárez-Bárcena, Emilio*: La utilización de la información, § VI Conclusiones [VI. Conclusions].

as the Netherlands, Italy or Germany.[175] The majoritarian position, according to *Bachmaier Winter*, prefers to ignore the activity of intelligence carried out by the intelligence services, and considers it as something that has nothing to do with the criminal procedure. She thinks that this is a dangerous position because it does not reflect reality at least in the field of the fight against terrorism, where the intelligence services play an important role. Not regulating the flood of information that enters the criminal procedure can put the guarantees of the criminal procedure and the fundamental rights of citizens in danger.[176] *Bachmaier Winter* does not advocate for a different standard of proof in these cases, but for the law to look for possible ways of facilitating the reproduction of evidence or the witness' testimony without endangering current operations against criminal organizations, always respecting the right to an effective remedy (article 6 ECHR).[177]

8. Concluding Remarks

In Spain, as in many other countries, the police forces and the intelligence service have joined their efforts in the fight against terrorism and organized crime. The preemptive focus in the fight against these types of crime has in some ways contributed to blurring the dividing line between police forces and intelligence services. The preemptive strategy against those serious crimes (and the criminalization of the previous stages of preparation of those type of crime) has driven the police to adopt intelligence methods in order to fight those crimes. In this regard, the Code of Criminal Procedure has incorporated new intrusive measures that serve the police to acquire that intelligence.[178] On the other hand, the law has conferred on the intelligence services an internal remit, which in the case of Spain is too broad (the CNI must protect, prevent, detect and enable the neutralization of those foreign services, groups or persons' activities that put at risk, threaten or attack the rights and freedoms of Spanish citizens), though in Spain this was not due to transnational terrorism, but to the threat of ETA.

Although in Spain police forces and the intelligence services still remain in different branches of government and have different structures, after 9/11 and especially the terrorist attacks in Madrid in 2004, the coordination between them has increased considerably in practice. As seen, the CNI already fought ETA terrorism and contributed to its eradication hand in hand with the police forces, but the fight against jihadist terrorism, with its transnational character, has meant a new step in the fight against terrorism and criminal organizations, involving the creation of new joint structures previously nonexistent. The creation of the CITCO is the best example of

---

175 *Bachmaier Winter, Lorena*: Información de inteligencia, pp. 63–69.

176 *Bachmaier Winter, Lorena*: Información de inteligencia, p. 63.

177 *Bachmaier Winter, Lorena*: Información de inteligencia, pp. 99–100.

178 On all this see, *Bachmaier Winter, Lorena*: Información de inteligencia, pp. 60–61.

this fact. The CITCO is a common structure where both bodies load the results of their terrorism and organized crime investigations that serve to coordinate efforts and operations. But while the practice reflects an increased coordination effort, the law regulating the coordination, and problems arising because of it, is still well behind the practice. The jurisprudence has had to confront some of these issues arising from this new scenario, but its answers to those problems cannot be said to be all-encompassing, and in some cases they have been influenced by the particular case that was brought before the court.[179]

List of Abbreviations

CESID	Centro Superior de Información para la Defensa (Superior Center of Information for Defense)
CCP	Code of Criminal Procedure (Ley de Enjuiciamiento Criminal or LECrim in Spanish)
CNI	Centro Nacional de Inteligencia (National Intelligence Service)
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
ECJ	European Court of Justice
LOPJ	Ley Orgánica del Poder Judicial (Judicial Power Organic Law)
SC	Spanish Constitution
SECED	Servicio Central de Documentación (Central Documentation Service)
SICOA	Coordination of Counter-terrorism Operations System
SRI/SCI	Investigations Registration System
STC	Judgment of the Constitutional Court
STS	Judgment of the Supreme Court

[179] In the case of the initiation of a criminal procedure on the base of the accusations made by the intelligence services, for example (as was the case seen in § 7.2) what would have happened if instead of an investigation of one of its own members after the discovery of a leak inside the CNI, the CNI would have come to the public prosecutor with a report accusing someone of being a terrorist after having carried out a security investigation of its own using its intrusive measures? Should we let the public prosecutor open a criminal investigation based on that information when normally criminal investigations are subject to different thresholds to those of the intelligence service (there must be a minimum degree of suspicion in order for the police to be able to use those intrusive measures; if the intelligence service can do that for them we will subvert all the system)? The law should establish if and when the information from the intelligence services can flow towards the criminal procedure [see on this *Bachmaier Winter, Lorena*: Información de inteligencia, p. 63].

Bibliography

Bachmaier Winter, Lorena: Información de inteligencia y proceso penal [Intelligence information and Criminal Procedure], in *Lorena Bachmaier Winter* (Coord.): Terrorismo y proceso penal y derechos fundamentales [Terrorism and Criminal Procedure and Fundamental Law], (2012), Marcial Pons, Madrid, pp. 45–101.

Bachmaier, Lorena & Del Moral García, Antonio: Criminal Law in Spain (2010), Wolters Kluwer.

Barcelona Llop, Javier: Policía y Constitución [Police and the Constitution], (1997), Tecnos.

Castillejo Manzanares, Raquel: La prueba pericial de inteligencia [The expert intelligence evidence] (2011), La Ley 19301/2011.

Catalina Benavente, María Ángeles: La unidad nacional de información sobre los pasajeros: el centro de inteligencia contra el terrorismo y el crimen organizado [The Passanger's National Unit: the Center against Terrorism and Organized Crime], in *Galán Muñoz, Alfonso & Mendoza Calderón, Silvia*: Globalización y lucha contra las nuevas formas de criminalidad transnacional [Globalization and the fight against the new transnational criminality], (2018), Tirant lo Blanch, Valencia, pp. 479–503.

De la Oliva Santos, Andrés; Aragoneses Martínez, Sara; Hinojosa Segovia, Rafael; Muerza Esparza, Julio; Tomé García, José Antonio: Derecho Procesal Penal [Criminal Procedural Law], (2007) 8th edition, Universitaria Ramón Arces, Madrid.

De la Oliva Santos, Andrés: El «control judicial previo» de la «inteligencia nacional» (O de cómo el *remedio* quizá resulta pero que la *enfermedad*) [The "previous judicial control" of the "national intelligence" (Or how sometimes the *remedy* is worse than the *illness*)] (2003), Tribunales de Justicia, pp. 1–20.

DeVine, Michael E.: Covert Action and Clandestine Activities of the Intelligence Community: Selected Definitions in Brief, (2019), Congressional Research Service Report (R45175).

Díez Fernández, Antonio M.: El servicio de inteligencia español a la luz de la teoría de las organizaciones [The Spanish intelligence Service under the light of organization theory], (2004), Cuadernos Constitucionales de la Cátedra Fabrique Furió Ceriol, n. 48, pp. 19–40.

Díaz Fernández, Antonio M.: El servicio de inteligencia: un actor político en la transición española [The intelligence service: a political actor in the Spanish Transition], (2005), Stud. hist., Hª cont., 23, pp. 201–219.

Díaz Fernández, Antonio M.: La adaptación de los servicios de inteligencia al terrorismo internacional [The adaptation of the intelligence services to international terrorism], (2006), Real Instituto Elcano, ARI Nº 52/2006.

Díaz Fernández, Antonio M.: Los servicios de inteligencia españoles. Desde la Guerra Civil hasta el 11-M. Historia de una transición [The Spanish Intelligence Services. From the Civil War to the 11-M. History of a transition], (2005), Alianza Editorial.

Expósito López, Lourdes: "El agente encubierto" [Cover agent], (2015), Revista de Derecho UNED, núm. 17, pp. 251–286.

Estrategia Española de Seguridad. Una responsabilidad de todos [Spanish Security Strategy. All's Responsibility], (2011), Gobierno de España.

Gimbernat Ordeig, *Enrique* "«La vida de nosotros», Estado de Derecho y Ley Penal" [Our life, Rule of Law and Criminal Law], (2009), La Ley, Madrid.

González Cussac, J.L.: "Intromisión en la intimidad y Centro Nacional de Inteligencia. Crítica al modelo español de control judicial previo" [Invasion of privacy and a critic to the Spanish model of prior judicial control], (2015), Revista Penal México, nº8, pp. 79–97.

González Navarro, Alicia: El uso de nuevas tecnologías en la investigación de delitos de terrorismo [The use of new technologies in the investigation of terrorism], (2018) *in Alonso Rimo, A, Cuerda Arnau, M.L., Fernández Hernández, A.:* Terrorismo, sistema penal y derechos fundamentales [Terrorism, criminal system and fundamental rights], Tirant lo Blanch, Valencia, pp. 543-578.

Gudín Rodríguez-Magariños, Faustino: La presunta prueba pericial de inteligencia: análisis de la STS de 22 de mayo de 2009 (1) [The supposed expert evidence: analysis of STS of 22nd May 2009], (2009), La Ley 17407/2009.

Hernandez Mosquera, Juan: "El servicio de información de la Guardia Civil (SIGC); 75 años de historia" [The information service of the Guardia Civil (SIGC); 75 years of history], (2016), Cuadernos de la Guardia Civil, 75 aniversario servicio de información, pp. 8–30.

James, Adrian: Examining Intelligence-Led Policing. Developments in Research, Policy and Practice, (2013), Palgrave Macmillan, London.

Llavador Piqueras, Javier and Llavador Cisternes, Hilario: El régimen jurídico de los servicios de inteligencia en España, (2015), Tirant lo Blanch, Valencia.

López-Barajas Perea, Inmaculada: La intervención de las comunicaciones electrónicas, (2011), La Ley, Madrid.

Martínez Sánchez, Juan Antonio: El reclutamiento de personal en el centro nacional de inteligencia (CNI) [Recruitment in the Spanish national intelligence center (CNI)], (2012), Papeles del Psicólogo, Vol. 33(3), pp. 202–210.

Oubiña Barbolla, Sabela: La proporcionalidad aplicada al acceso de datos personales conservados por los operadores de servicios de comunicaciones [The proportionality principle applied to the access of personal data retained by communications service operators], (2019), Thomson Reuters Aranzadi, pp. 303–335.

Parejo Alfonso, Luciano: Seguridad Pública y policía administrativa de seguridad. Problemas de siempre y de ahora para el deslinde, la decantanción y la eficacia de una responsabilidad nuclear del Estado administrativo [Public Security and Administrative Police], (2008), Tirant lo Blanch, Valencia.

Pérez Villalobos, Mª Concepción: Derechos fundamentales y servicios de inteligencia (un estudio a la luz de la nueva legislación) [Fundamental rights and intelligence services (a study taking into account the new regulation], (2002), Biblioteca de Derechos Fundamentales, Grupo Editorial Universitario, Granada.

Rodríguez Lainz, José Luis: El Régimen Legal español en materia de conservación y cesión de datos para la investigación de delitos [The Spanish Legal Regime on the Conservation and Transfer of Data for The Investigation of Crimes], (2018), Diario La Ley, nº 9291 (sección Doctrina).

Ruíz Miguel, Carlos: El CESID: Historia de un intento de modernización de los Servidos de Inteligencia [The CESID: History of an attempt to modernize the Intelligence Service], (2005), Arbor CLXXX, 709, pp. 121–150.

Schaible, Lonnie M. and Sheffield, James: "Intelligence-led policing and change in state law enforcement agencies", (2012), Policing: An International Journal of Police Strategies & Management, Vol. 35 No. 4, pp. 761–784.

Tejerina Rodríguez, Ofelia: Seguridad del Estado y Privacidad [State Security and Privacy], (2014), ed. Reus, Madrid.

The 9/11 Commission Report. Final Report of the National Commission on Terrorist Attacks Upon the United States (2004).

Grundzüge der inneren Sicherheitsarchitektur in der Türkei

Insbesondere die Verbrechensbekämpfung durch die Nachrichtendienste

Mehmet Arslan und Erdem Izzet Külçür

Einführung

Das Sicherheitsrecht ist in der Türkei eine relativ neue Disziplin. Als etwa Yeniseys Lehrbuch über das Polizeirecht (kolluk hukuku) 2009 in seiner ersten Auflage erschien, füllte es nicht nur eine bestehende Lücke, sondern erfuhr auch deshalb Aufmerksamkeit, weil sich hier ein Strafrechtler mit dem Polizeirecht auseinandersetzte.[1] Über viele Grundbegriffe, wie z.B. den der Gefahr, besteht bis heute weder im Gesetzesrecht noch in der Praxis Klarheit. Dies gilt erst recht für das Sicherheitsrecht im weiteren Sinne, das auch das Recht der Nachrichtendienste einschließt. Eine systematische Erfassung des inneren Sicherheitsrechts fehlt immer noch und somit ist dieser neue Rechtsbereich stark entwicklungsbedürftig. Im vorliegenden Beitrag wird der Versuch unternommen, die bestehenden Gesetze zu interpretieren und

[1] Mittlerweile ist das Buch in zweiter Auflage erschienen: *Yenisey*, Kolluk Hukuku [Polizeirecht], Istanbul 2015.

Fragen zusammenzutragen, die dringend einer Klärung bedürfen. Im Zentrum steht die Verbrechensbekämpfung durch die Nachrichtendienste.

Der Beitrag gliedert sich in drei Hauptteile. Der erste Teil befasst sich mit den sicherheitsbehördlichen Aufgabenfeldern (I.). Dabei werden nicht nur die Organisation der türkischen Nachrichtendienste, deren Aufgaben und Befugnisse dargestellt (I.A), sondern auch die strafverfolgungsrelevanten Aufgabenfelder der Dienste aufgezeigt (I.B). Im zweiten Teil wird auf die Interaktion zwischen den Nachrichtendiensten und der Strafverfolgung gesondert eingegangen (II.). Der dritte Teil stellt nach einem allgemeinen Überblick (III.A) dar, inwiefern die nachrichtendienstlichen Informationen an die Strafverfolgung übermittelt werden dürfen (III.B) und wie und unter welchen Voraussetzungen diese Informationen im Ermittlungs- und Hauptverfahren Verwendung finden (III.C). Der Beitrag schließt mit einer Zusammenfassung.

I. Sicherheitsbehördliche Aufgabenfelder

Sowohl der strukturelle Aufbau der Sicherheitsbehörden als auch das entsprechende Regelwerk dieser Behörden in der Türkei lässt eine funktionale Aufgabenteilung in drei Bereiche erkennen: nachrichtendienstliche Tätigkeiten (istihbarat), polizeiliche Gefahrenabwehr/Prävention (önleme) und Strafverfolgung (ceza takibi). Für die Gefahrenabwehr sind Polizei[2] und Gendarmerie[3] zuständig. Die Strafverfolgung liegt im Zuständigkeitsbereich der Staatsanwaltschaft,[4] der die Ermittlungspersonen der Polizei oder der Gendarmerie bei der Aufklärung und Verfolgung von Straftaten per Gesetz unmittelbar unterstellt sind.[5] Polizei und Gendarmerie sind beide Polizeibehörden (kolluk). Während die Polizei grundsätzlich in den Städten tätig ist, erfüllt die Gendarmerie die polizeibehördlichen Aufgaben auf dem Land.[6]

---

[2] § 2 Abs. 1A des Gesetzes über Aufgaben und Befugnisse der Polizei [*Polis Vazife ve Selahiyet Kanunu* (im Folgenden zitiert: PVSK)], Gesetz-Nr. 2559 vom 04.07.1934, veröffentlicht im Amtsblatt vom 14.07.1934, Nr. 2751.

[3] § 7 Abs. 1 lit. a des Gesetzes über Organisation, Aufgaben und Befugnisse von Gendarmerie [*Jandarma Teşkilat, Görev ve Yetkileri Kanunu* (im Folgenden zitiert: JTGYK)], Gesetz-Nr. 2803 vom 10.03.1983, veröffentlicht im Amtsblatt vom 12.03.1983, Nr. 17985.

[4] § 160 Abs. 1 Türkische Strafprozessordnung, hierzu siehe *Arslan*, Einführung und Übersetzung, S. 176.

[5] § 2 Abs. 1B. PVSK; § 7 Abs. 1 lit. b. JTGYK.

[6] Siehe § 12 Abs. 1 des Gesetzes über die Organisation der Polizei [*Emniyet Teşkilat Kanunu* (im Folgenden zitiert: ETK)], Gesetz-Nr. 3201, vom 04.06.1937, veröffentlicht im Amtsblatt vom 12.06.1937, Nr. 3629.

A. Organisation der Nachrichtendienste

Grundsätzlich besteht eine organisatorische Unterscheidung zwischen dem Nachrichtenwesen der Nationalen Sicherheit (*national security intelligence*) und dem Nachrichtenwesen der Gesetzvollzugsbehörden (*law enforcement intelligence*). Im Bereich der Nationalen Sicherheit sind der Nationale Nachrichtendienst (Milli İstihbarat Teşkilatı: im Folgenden MIT)[7] und die Nachrichtendienstdirektion des Generalstabs (Genelkurmay İstihbarat Daire Başkanlığı: im Folgenden GIDB) tätig. Hingegen sind die Nachrichtendienstdirektion der Polizei (Emniyet İstihbarat Daire Başkanlığı: im Folgenden EIDB)[8] und das Nachrichtendienstpräsidium der Gendarmerie (Jandarma İstihbarat Başkanlığı: im Folgenden JIB)[9] mit den nachrichtendienstlichen Tätigkeiten im Bereich der Gesetzvollzugsbehörden betraut.

Die Aufklärung zum Zwecke der nationalen Sicherheit erfolgt grundsätzlich durch den MIT, wobei dieser nur in geringem Umfang Kompetenzen zur militärischen Aufklärung innehat. Er darf weder abschirmdienstliche Tätigkeiten innerhalb des Militärs ausüben, noch ist er an der strategischen Aufklärung für das Militär beteiligt.[10] Diese führt die Nachrichtendienstdirektion des Generalstabs (GIDB) selbst durch.[11] Der MIT ist allerdings damit beauftragt, entsprechend einer Vereinbarung dem Generalstab die Informationen zu liefern, die Letzterer für die Streitkräfte als erforderlich erachtet.[12]

Der MIT ist unmittelbar dem Staatspräsidenten unterstellt,[13] während die GIDB dem Verteidigungsministerium,[14] die EIDB und das JIB dem Innenministerium[15]

---

[7] §§ 4, 6 des Gesetzes über die nachrichtendienstlichen Dienste des Staates und den Nationalen Nachrichtendienst (MIT-Gesetz), [*Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanunu*], Gesetz-Nr. 2937, vom 01.11.1983, veröffentlicht im Amtsblatt vom 03.11.1983, Nr. 18210; siehe diese Vorschriften im Anhang Gesetzestexte.

[8] Zusatzparagraph 7 PVSK; siehe diese Vorschrift im Anhang Gesetzestexte.

[9] § 7 Abs. 1 lit. a. JTGYK.

[10] Auch wenn das die Vorgabe ist, so können die Militärbehörden dem MIT oder auch einem anderen Dienst erlauben, Informationen innerhalb ihrer Behörde oder hinsichtlich ihres Personals zu sammeln. In der Tat existieren laut Medienberichten entsprechende Protokolle zwischen dem Generalstab und dem MIT. (Aufgrund § 4 Abs. 1 lit. e des MIT-Gesetzes). Das Protokoll soll wie folgt heißen: *T.S.K. İstihbarata Karşı Koyma, Koruyucu Güvenlik ve İşbirliği Yönergesi, MY: 114-1(C)*. Für die entsprechende Pressemeldung siehe https://www.timeturk.com/my-114-1-mit-e-tsk-da-istihbarat-yapma-yetkisi-veren-yonerge/haber-686835.

[11] *Fidan*, Intelligence and Foreign Policy, S. 64, 67–68.

[12] § 4 Abs. 1 lit. e des MIT-Gesetzes; im Jahr 2012 wurde der MIT mit der elektronischen Nachrichtensammlung von der Generalstab der Elektroniksystem-Kommandantur (GES – Genelkurmay Elektronik Sistemler Komutanlığı) beauftragt. Siehe die Antwort des Verteidigungsministers auf die Anfrage https://www2.tbmm.gov.tr/d24/7/7–8252c.pdf.

[13] § 3 Abs. 1 des MIT-Gesetzes.

[14] § 1 Abs. 1, 2a des Gesetzes über die Aufgaben und Befugnisse des Generalstabschefs, [*Genelkurmay Başkanının Görev ve Yetkilerine Ait Kanun*], Gesetz-Nr. 1324, vom 31.07.1970, veröffentlicht im Amtsblatt vom 07.08.1970, Nr. 13572.

[15] § 4 JTGYK; § 1 ETK.

untergeordnet sind. Ein eigenes Gesetz über die Organisation, nachrichtendienstliche Aufgaben sowie Befugnisse besteht allerdings lediglich für den MIT. Die Nachrichtendienstdirektion des Generalstabs (GIDB) verfügt nicht über ein entsprechendes eigenes Gesetz.[16] EIDB und das JIB sind dagegen nur im Hinblick auf ihre Aufgaben bzw. auf ihre Befugnisse[17] in allgemeinen Gesetzen über die Polizei und Gendarmerie geregelt. Insofern fehlt ebenfalls ein besonderes Gesetz über die Organisation dieser Dienste.

Der MIT ist gleichzeitig der Dachverband der zivilen Nachrichtendienstbehörden. Er ist sowohl im Ausland als auch im Inland tätig. Das wird zuweilen beanstandet, insbesondere unter dem Aspekt, dass der MIT dadurch andere Aufgabenbereiche, allen voran die Auslandsaufklärung, vernachlässige.[18] Es gibt also keine zwei unterschiedlichen Dienste für das Aus- und Inland in der Türkei, wie den Bundesnachrichtendienst (BND) und das Bundesamt für Verfassungsschutz (BfV) in Deutschland.[19] Weitere Inlandsdienste sind die Nachrichtendienstdirektion der Polizei (EIDB) und das Nachrichtendienstpräsidium der Gendarmerie (JIB). Diese drei Behörden sind die Hauptproduzenten nachrichtendienstlicher Informationen in der Türkei. Im Inland sind deswegen in einigen Bereichen einschließlich des Staats- und Verfassungsschutzes (hierzu unten mehr) alle Nachrichtendienste tätig. Dieser Zustand hat durchaus das Potenzial, Konflikte zu verursachen, weil mehrere Behörden in ein und denselben Sachverhalt involviert sein können, ohne dass sie sich absprechen müssen.

Zu den obengenannten Diensten kommt die Kommission zur Ermittlung von Finanzkriminalität (Mali Suçları Araştırma Kurulu: im Folgenden MASAK) hinzu. Die MASAK ist organisatorisch innerhalb des Finanzministeriums angesiedelt. Ob diese Behörde ein Finanznachrichtendienst ist, lässt sich nicht eindeutig beurteilen, wobei sich die Behörde selbst als die „Finanznachrichtendiensteinheit der Türkei“ und ihre Aufgabenart zunehmend als nachrichtendienstlich (istihbari) bezeichnet.[20] Da die Informationssammlung durch die MASAK, jedenfalls gegenwärtig, auf eine antizipierte spätere Verfolgung bestimmter Straftaten zugeschnitten scheint, wird sie unten im Zusammenhang mit den strafverfolgungsrelevanten Aufgabenfeldern der Dienste erörtert.

---

[16] Im Rahmen der Aufgaben und Befugnisse des Generalstabschefs wird nur lapidar erwähnt, dass er sicherstellen muss, dass der militärische Nachrichtendienst zum Zug kommt. Siehe § 2 Abs. 2 lit. a des Gesetzes über die Aufgaben und Befugnisse des Generalstabchefs.

[17] Hierzu mehr siehe unten I.A.2.a) zu den Aufgaben der EIDB und des JIB.

[18] Das hat auch der amtierende Präsident des Nachrichtendienstes (MIT), Hakan Fidan, bereits 1999 zum Ausdruck gebracht; siehe *Fidan*, Intelligence and Foreign Policy, S. 79 ff.

[19] Dazu mehr *Arslan*, Intelligence and Crime Control, S. 513 ff.

[20] Sie bezeichnen sich selbst auf ihrer Webseite als „die Finanznachrichtendiensteinheit der Türkei” http://www.masak.gov.tr/tr/default.

Zudem existiert ein Koordinationsgremium des nationalen Nachrichtenwesens (Milli İstihbarat Koordinasyon Kurulu: MİKK).[21] Der MIT ist gesetzlich zuständig für die Koordination zwischen nachrichtendienstlichen Behörden soweit es entsprechende Informationssammlungen betrifft. Ob und wie dieses Gremium Absprachen und den Austausch von Informationen zwischen den Diensten vornimmt, ist nicht näher öffentlich bekannt.

1. Nationaler Nachrichtendienst (MIT)

Das MIT-Gesetz unterscheidet ausdrücklich zwischen Aufgaben und Befugnissen der Behörde.[22] Zwar enthalten die Aufgaben- und Befugnisnormen noch klärungsbedürftige Begriffe, Verweise auf nichtgesetzliche Verwaltungsvorschriften sowie unspezifische und generalklauselartige Ermächtigungsgrundlagen, dennoch verbietet das Gesetz explizit, dem MIT andere Aufgaben zu übertragen, als die, die dieses Gesetz vorsieht.[23]

a) Aufgaben des MIT

Schaut man sich die Aufgaben an, so lässt sich feststellen, dass die Hauptaufgabe des MIT darin besteht, nachrichtendienstliche Erkenntnisse für die nationale Sicherheit zu generieren.[24] Diese beziehen sich auf die existierenden oder möglichen Aktivitäten von innen oder außen, die sich gegen bestimmte hochrangige Güter des Landes richten. Die genannten Güter sind die Integrität der Türkischen Republik als Land und als Nation, deren Bestand, Unabhängigkeit, Sicherheit, Verfassungsordnung sowie alle Bestandteile der nationalen Schlagkraft.[25] Klassisch nachrichtendienstlich tätig ist der MIT auch bei der Vornahme von Maßnahmen gegen Spionage.[26]

Grundsätzlich liegt der Zweck der nachrichtendienstlichen Generierung von Erkenntnissen für die nationale Sicherheit darin, diese den politischen und militärischen Organen (i.e. dem Staatspräsidenten, dem Generalstabchef und dem Sekretär

---

[21] Das Staatssekretariat für Öffentliche Ordnung und Sicherheit (KDGM – Kamu Düzeni ve Güvenliği Müsteşarlığı) ist durch den § 124 des Präsidialdekrets Nr. 703 abgeschafft worden.

[22] §§ 4 und 6 des MIT-Gesetzes; siehe diese Vorschriften im Anhang Gesetzestexte.

[23] § 4 Abs. 1 des MIT-Gesetzes.

[24] Der Begriff der nationalen Sicherheit wurde im Jahr 1970 vom Obersten Verwaltungsgericht der Türkei [*Danıştay*] wie folgt definiert: „die Gewährleistung der Sicherheit und der Verteidigung des Staats gegen die inneren bzw. äußeren Gefahren, die landesweit in Erscheinung treten." Danıştay 12. D., T: 05.03.1970, E: 1969/4097, K: 1970/426. Für das Urteil siehe *Aybay*, AÜSBFD 1978, 69.

[25] § 4 Abs. 1 lit. a des MIT-Gesetzes.

[26] § 4 Abs. 1 lit. g des MIT-Gesetzes.

des Nationalen Sicherheitsrats) sowie anderen betreffenden Behörden von sich aus oder auf Anfragen und entsprechend deren Bedürfnissen zur Verfügung zu stellen sowie die genannten Stellen bei der Entwicklung und Durchführung der nationalen Sicherheitspolitik mit Vorschlägen und beim Schutz vor Spionage durch technische Beratung und Koordination zu unterstützen.[27] Allerdings ist der MIT neben seiner genuinen Aufgabe der Informationssammlung und Entwicklung des *national security intelligence* auch damit beauftragt, anderweitige Aufgaben wahrzunehmen, die der Nationale Sicherheitsrat (Milli Güvenlik Kurulu: MGK) ihm überträgt.[28] Ob damit auch Aufgaben gemeint sind, die über die reine Informationssammlung hinausgehen, ist nicht geklärt. Spätestens seit der Gesetzesänderung 2014 scheint der MIT Aufgaben der genannten Art erhalten zu haben. Die Behörde ist nämlich nun dazu angehalten, Anweisungen des Staatspräsidenten Folge zu leisten, wenn diese die Angelegenheiten der äußeren Sicherheit, die Terrorismusbekämpfung sowie die nationale Sicherheit betreffen.[29] Da diese Bereiche bereits einen Ausschnitt der obengenannten nationalsicherheitsrelevanten Felder ausmachen und der MIT die diesbezügliche Informationssammlung in erster Linie nach der obengenannten allgemeinen Aufgabennorm vornehmen wird, umfasst die neue Aufgabenorm aus dem Jahr 2014 wohl Handlungen, die sich nicht in der Informationssammlung erschöpfen. Ob damit auch exekutive Aufgaben gemeint sind, die der MIT unmittelbar eigenhändig ausführen darf, ist nicht geklärt. Entsprechende Hinweise, die teils die Bejahung dieser Frage nahelegen, lassen sich jedoch aus einigen Befugnisnormen ableiten, auf die sogleich unten einzugehen ist.

Neu ist seit der genannten Gesetzesänderung von 2014 auch, dass der MIT ausdrücklich mit dem *law enforcement intelligence* im Hinblick auf bestimmte Kriminalitätsfelder betraut ist. Da dies mit den entsprechenden Tätigkeiten der anderen Dienste der Polizei und der Gendarmerie eng zusammenhängt, wird es im Folgenden gesondert erörtert.

b) Befugnisse des MIT

Wie bereits hervorgehoben, sind die Befugnisse des MIT bei der Erfüllung der obengenannten Aufgaben gesondert geregelt. Diese Unterscheidung macht deutlich, dass dem Gesetz das Prinzip zugrunde liegt, dass aus den Aufgabennormen per se keine Befugnisse abzuleiten sind. Anzumerken ist an dieser Stelle, dass die Grundrechtseingriffe durch die Maßnahmen des MIT verfassungsrechtlich stets eines Parlamentsgesetzes bedürfen.[30] Diesem verfassungsrechtlichen Gebot kommt das MIT-

---

[27] § 4 Abs. 1 lit. a, b, c, und d des MIT-Gesetzes.

[28] § 4 Abs. 1 lit. f des MIT-Gesetzes.

[29] § 4 Abs. 1 lit. h des MIT-Gesetzes.

[30] Art. 13 Abs. 1 türkischer Verfassung.

Gesetz mit einer Generalklausel[31] sowie mit der ausdrücklichen Ermächtigung zu einzelnen nachrichtendienstlichen Ermittlungsmaßnamen nach. An dieser Stelle werden von den ausdrücklich genannten Maßnahmen einige wichtige genannt, wobei deren Voraussetzung im vorliegenden Beitrag im Detail nicht ausgeführt werden kann (siehe § 6 des MIT-Gesetzes im Anhang Gesetzestexte):

– Erhebung von Informationen bei öffentlichen Stellen oder privaten Personen einschließlich der Banken,[32]
– Nutzung von Legenden, Gründung juristischer Personen, Ausstellung von Papieren sowie Dokumenten,[33]
– Überwachung des Telekommunikationsverkehrs durch die Suche nach Angaben, die das Ausland, die nationale Verteidigung, den Terrorismus, internationale Straftaten[34] sowie die Cyber-Sicherheit betreffen (strategische Telekommunikationsüberwachung),[35]
– Feststellen und Abhören der Telekommunikation von Einzelnen für einen bestimmten Zeitraum und Speichern der Inhalte sowie die Auswertung der Verkehrsdaten, wenn bestimmte Verfassungswerte ernsthaft bedroht sind (individuelle Telekommunikationsüberwachung),[36]
– Unabhängig von den beiden genannten Arten der Telekommunikationsüber wachung, Feststellen und Abhören der Telekommunikation im Ausland, von Ausländern und/oder aus den Münzfernsprechern und Speichern der Inhalte sowie die Auswertung der Verkehrsdaten (Ausland-Ausland-, Ausländer- und anonyme Telekommunikationsüberwachung).[37]

Besondere Beachtung verdienen die obengenannten verschiedenen Überwachungsbefugnisse des MITs, die 2005 und 2014 gesetzlich eingeführt wurden. Diese Massenüberwachungsmaßnahmen stehen offenkundig im Einklang mit den entsprechenden Tendenzen in anderen Ländern.[38]

---

[31] Nach § 6 Abs. 1 lit. d des MIT-Gesetzes kann der MIT zur Erfüllung seiner Aufgaben von verdeckten Vorgehens- und Arbeitsweisen sowie Techniken Gebrauch machen.

[32] § 6 Abs. 1 lit. b des MIT-Gesetzes.

[33] § 6 Abs. 1 lit. e des MIT-Gesetzes.

[34] Wie der Begriff internationaler Straftaten zu verstehen ist und ob und inwiefern diese sich von grenzüberschreitenden Straftaten unterscheiden, ist nicht klar. Für eine Auseinandersetzung mit den diesbezüglichen begrifflichen Unterschieden siehe *Külçür*, SCD 2016, 7 ff.

[35] § 6 Abs. 1 lit. g des MIT-Gesetzes.

[36] § 6 Abs. 2 bis 9 des MIT-Gesetzes.

[37] § 6 Abs. 10 des MIT-Gesetzes. Für eine rechtsphilosophische Auseinandersetzung mit der weltweiten Telekommunikationsüberwachung durch Nachrichtendienste siehe *Arslan*, KritV 2018, 287 ff.

[38] Hierzu siehe *Arslan*, KritV 2018/4, 287 ff.

Wie bereits oben erwähnt, ist die Frage nicht vollständig geklärt, ob der MIT jedenfalls seit der Gesetzesänderung in 2014 nun mit Aufgaben beauftragt ist, die über die bloße Informationssammlung zum Zwecke der Generierung von Erkenntnissen für die nationale Sicherheit hinausgehen. In diesem Zusammenhang ist eine besondere Befugnis des MITs zu sehen, wonach der MIT mit einheimischen oder ausländischen Körperschaften, Einrichtungen aller Art (her türlü), allen (tüm) Vereinigungen, Zusammenschlüssen oder Personen unmittelbar in Kontakt treten und in diesen Zusammenhängen von einschlägigen Koordinationsmaßnahmen Gebrauch machen kann.[39] Da sich die Vorschrift nach dem Wortlaut auf *alle* (tüm) Vereinigungen bezieht, lässt sich daraus entnehmen, dass der MIT neuerdings auch befugt ist, Gespräche auch mit illegalen einschließlich terroristischer Vereinigungen[40] zu führen.[41]

In der Zusammenschau dieser Befugnis und der obengenannten Aufgabennormen hinsichtlich der vom Nationalen Sicherheitsrat übertragenen Aufträge sowie der vom Staatspräsidenten erteilten Anweisungen ist davon auszugehen, dass der MIT nun auch mit einigen bestimmten operativen Aufgaben beauftragt ist, die klar über die nachrichtendienstliche Informationssammlung hinausgehen. Dennoch ist noch die Frage zu beantworten, ob und welche eventuell exekutiven Befugnisse den MIT-Angehörigen zustehen, die sie bei einer unmittelbaren eigenhändigen Ausführung operativer Aufgaben heranziehen könnten und unmittelbaren Zwang umfassen.

Einschlägig könnte in der Hinsicht § 6 Abs. 13 des MIT-Gesetzes sein, wonach durch eine Rechtsverordnung zu regeln ist, welche MIT-Angehörige von den Rechten und den Befugnissen der (allgemeinen) Polizei während der Erfüllung der in diesem Gesetz festgehaltenen Aufgaben Gebrauch machen dürfen. Es lässt sich allerdings argumentieren, dass diese exekutiven Befugnisse lediglich dafür eingeräumt sind, um die Behörde selbst oder deren Angehörige durch ihr eigenes Personal zu schützen. Dafür spricht insbesondere, dass die Vorschrift in ihrem Wortlaut ausdrücklich den Begriff „während der Erfüllung der in diesem Gesetz genannten Aufgaben“ (Bu Kanunda yazılı görevlerin yerine getirilmesi sırasında) und nicht „zur Erfüllung“ (yerine getirilmesi amacıyla) verwendet. Vertretbar ist insofern etwa, dass der MIT beispielsweise bei der Gegenspionage im Inland zum eigenen Schutz von allgemeinen polizeilichen Zwangsbefugnissen, etwa Schusswaffen nach

---

[39] § 6 Abs. 1 lit. a des MIT-Gesetzes.

[40] Siehe auch § 6 Abs. 1 lit. j des MIT-Gesetzes, wonach MIT-Angehörige bei der Erfüllung ihrer Aufgaben verhaftete und verurteilte Personen, die sich in Justizvollzugsanstallten befinden, nach einer vorausgehenden Benachrichtigung besuchen, andere Personen zum Besuch mitbringen und alle Zusammenschlüsse einschließlich der Terrororganisationen, die die nationale Sicherheit bedrohen, kontaktieren dürfen.

[41] Anderer Ansicht ist *Yenisey*. Nach ihm sind mit Organisationen lediglich die legalen gemeint. So wie der Verdeckte Ermittler gemäß § 139 Abs. 5 tStPO bei der Ausführung seines Auftrags keine Straftat begehen darf, dürfe die Kontaktaufnahme oder auch der Gebrauch von Koordinationsmethoden nicht zur Begehung von Staftaten führen. Die genannten Handlungen seitens der MIT-Angehörigen könnten aber die Beteilung an entsprechenden Straftaten begründen, so *Yenisey*, Kolluk Hukuku, S. 377.

§ 6 Abs. 13 des MIT-Gesetzes i.V.m § 16 Abs. 2 des Polizeigesetzes (PVSK) Gebrauch macht.

Insofern lassen sich aus § 6 Abs. 13 des MIT-Gesetzes keine allgemeinen exekutiven Befugnisse für den MIT ableiten, die der Behörde bei der unmittelbaren Erfüllung der obengenannten vom Sicherheitsrat oder Staatspräsidenten erteilten Aufträge und Anweisungen zur Verfügung stehen könnten. Im Ergebnis ist festzustellen, dass der MIT 2014 jedoch mit einer neuen Aufgabe ausgestattet worden ist (Erfüllung präsidialer Anweisungen). Korrespondierende Befugnisnormen (abgesehen von der Führung von Gesprächen mit illegalen einschließlich terroristischen Vereinigungen und der Durchführung der Koordinationsmaßnahmen), insbesondere exekutive, die den MIT zur Anwendung unmittelbaren Zwangs ermächtigen würden, sind jedoch ins MIT-Gesetz nicht eingeführt worden. Dies schließt allerdings nicht aus, dass sich der MIT durch das Bereitstellen von Informationen sowohl im Inland als auch im Ausland an der Anwendung unmittelbaren Zwangs durch die operativen tätigen Polizeibehörden oder auch Streitkräfte beteiligt.

2. Nachrichtendienstdirektion der Polizei (EIDB) und der Gendarmerie (JIB)

Wie bereits oben erwähnt werden die inlandsnachrichtendienstlichen Aufgaben neben dem MIT auch von der Nachrichtendienstdirektion der Polizei (EIDB) und dem Nachrichtendienstpräsidium der Gendarmerie (JIB) wahrgenommen. Sowohl die Aufgaben als auch die Befugnisse sind jeweils im Zusatzparagraph 7 des Polizeigesetzes und im Zusatzparagraph 5 des Gendarmeriegesetzes geregelt (siehe die Vorschriften im Anhang Gesetzestexte).

a) Aufgaben der EIDB und des JIB

Die hochrangisten Güter, die durch die nachrichtendienstliche Tätigkeit der EIDB zu schützen sind, sind die Integrität der Türkischen Republik als Land und als Nation, die Verfassungsordnung sowie die öffentliche Sicherheit, soweit sich dies auf das Inland bezieht (Staats- und Verfassungsschutz).[42] Das Polizeigesetz macht klar, dass im Gegensatz zur Bereitstellung von Informationen durch den MIT für die Entwicklung einer nationalen Sicherheitspolitik der Gegenstand der polizeibehördlichen nachrichtendienstlichen Tätigkeiten die Herstellung der öffentlichen Sicherheit und Ordnung ist.[43] In Hinblick auf das JIB hingegen enthält das Gesetz keinen allgemeinen Auftrag zum Schutz bestimmter hochrangiger Güter des Landes durch die

---

[42] Siehe Zusatzparagraph 7 Abs. 1 des PVSK; siehe auch Zusatzparagraph 7 Abs. 2 des PVSK Zusatzparagraph und 5 Abs. 1 des JTGYK. Beide Vorschriften schließen ausdrücklich die Informationssammlung hinsichtlich der Spionagestraftaten seitens der Inlandsdienste aus.

[43] Zusatzparagraph 7 Abs. 1 des PVSK; siehe die Vorschrift im Anhnag Gesetzestexte.

nachrichtendienstlichen Tätigkeiten.[44] Es wird nachrichtendienstlich nur tätig, um die Begehung bestimmter schwerer Katalogstraftaten zu verhindern.[45] Das Fehlen einer allgemeinen Aufgabennorm impliziert, dass das JIB im Vergleich zum EIDB als Inlandsdienst eine sekundäre Rolle zugewiesen ist.[46]

b) Befugnisse der EIDB und des JIB

Der Zusatzparagraph 7 Abs. 1 des Polizeigesetzes (PVSK) sieht ausdrücklich vor, dass zum Zwecke der nachrichtendienstlichen Tätigkeiten (istihbarat faaliyetleri amacıyla) Informationen zu sammeln (toplar) und auszuwerten (değerlendirir) sind.[47] Unklar ist jedoch, ob diese Vorschrift lediglich den Aufgabenbereich der EIDB beschreibt oder doch darüber hinaus eine Befugnisnorm enthält. In Anbetracht der Tatsache, dass eine solche Trennung im durchaus sehr jungen türkischen Polizeirecht nicht geläufig ist, ist davon auszugehen, dass man, jedenfalls in der Praxis, aus dem Zusatzparagraph 7 Abs. 1 des Polizeigesetzes auch eine Generalklausel zur Ermächtigung nachrichtendienstlicher Maßnahmen entnimmt.[48] Wie bereits oben erwähnt, fehlt im Gendarmeriegesetz für das JIB nicht nur eine allgemeine Aufgabennorm, sondern auch eine entsprechende Generalklausel. Deswegen ist davon auszugehen, dass das JIB zum Zwecke der Informationssammlung für die Vorbeugung schwerer Straftaten nur dann auf eine Befugnis zurückgreifen kann, wenn diese ausdrücklich im Gesetz genannt ist. Betrachtet man das Polizei- und Gendarmeriegesetz, so stehen den beiden Inlandsnachrichtendiensten EIDB und JIB folgende Maßnahmen zu:

– Erhebung von Informationen bei öffentlichen Stellen,[49]
– Observation durch technische Mittel,[50]
– Feststellen, Abhören, Speichern der Telekommunikation von Einzelnen sowie Auswertung der Verkehrsdaten.[51]

---

[44] Siehe Zusatzparagraph 5 Abs. 1 des JTGYK; siehe die Vorschrift im Anhang Gesetzestexte.

[45] Siehe Zusatzparagraph 5 Abs. 1 des JTGYK; für diese Straftaten siehe unten I.B.1. MIT, EIDB und JIB.

[46] Dass das JTGYK im Vergleich zum PVSK das speziellere Gesetz darstellt, und das letztere für das Polizeirecht das allgemeinere Gesetz ist, zeigt sich auch dadurch, dass die polizeibehördlichen Ermächtigungsgrundlagen zum Ergreifen von einzelnen Maßnahmen grundsätzlich im PVSK geregelt sind. Diese Befugnisse stehen nach § 25 Abs. 1 PVSK auch der Gendarmerie zu.

[47] Siehe Zusatzparagraph 7 Abs. 1 des PVSK.

[48] Ob und inwiefern dies sich mit dem verfassungsrechtlichen Gesetzesvorbehalt bei Grundrechtseingriffen nach Art. 13 tVerf. vereinbaren lässt, kann an dieser Stelle nicht erörtert werden.

[49] Siehe Zusatzparagraph 7 Abs. 6 des PVSK; Zusatzparagraph 5 Abs. 5 des JTGYK.

[50] Siehe Zusatzparagraph 7 Abs. 6 des PVSK; Zusatzparagraph 5 Abs. 5 des JTGYK.

[51] Siehe Zusatzparagraph 7 Abs. 2 des PVSK; Zusatzparagraph 5 Abs. 1 des JTGYK.

Zur Überwachung des Datenverkehrs zwischen einzelnen IP-Adressen und Internetquellen ist dagegen nur die Nachrichtendirektion der Polizei befugt.[52]

c) Abgrenzung zwischen der nachrichtendienstlichen Informationssammlung, Gefahrenabwehr und Strafverfolgung im türkischen Inlandsnachrichtendienst

Das türkische Polizei- und Gendarmerierecht kennt zwei Aufgabenarten: Prävention (önleyici, mülki-idari) und Repression (adli).[53] Während sich die repressiven Tätigkeiten auf die bereits zumindest versuchten, begangenen Straftaten einschließlich der fortgesetzten beziehen,[54] so besteht im türkischen Recht kein allgemein definierter Anknüpfungspunkt für das Tätigwerden der Polizei und der Gendarmerie im Bereich der Prävention, etwa eine bestimmte Art und Grad der Gefahr, der sich gegen die polizeirechtlich geschützten Rechtsgüter richtet oder diese beeinträchtigen würde. Im Gegensatz dazu beschreiben die Gesetze die Prävention pauschal als eine behördliche Vorgehensweise, die darin besteht, der Begehung normwidriger Handlungen im Voraus vorzubeugen[55] oder Maßnahmen zu treffen, um die Begehung von Straftaten zu verhindern.[56] Das Fehlen eines allgemein definierten Anknüpfungspunkts bzw. einer Eingriffsschwelle führt nicht zuletzt dazu, dass die polizeibehördliche Prävention nicht nur die Gefahrenabwehr in einem Einzelfall, sondern auch die nachrichtendienstliche Informationssammlung der Behörden in Hinblick auf unspezifische mögliche Gefahren bzw. Bedrohungen umfasst, da auch diese Informationssammlung im weiteren Sinne unter die Vorbeugung normwidriger Handlungen bzw. die Verhütung von Straftaten fällt.[57]

Das allgemeine türkische Polizeirecht (kolluk hukuku) enthält einen breiten Katalog von einzelnen Maßnahmen, die die Polizei und Gendarmerie gegen Personen zum Zwecke der Gefahrenabwehr ergreifen dürfen.[58] Hierzu gehören etwa das Anhalten und die Ausweiskontrolle,[59] die Durchsuchung von Personen, Fahrzeugen, Sachen und Dokumenten,[60] die Festnahme und Platzverweise[61] oder die Abnahme

---

[52] Siehe Zusatzparagraph 7 Abs. 2 des PVSK.

[53] § 2 Abs. 1 des PVSK und § 7 Abs. 1 des JTGYK.

[54] § 2 Abs. 1A des PVSK und § 7 Abs. 1 lit. a des JTGYK.

[55] § 2 Abs. 1A des PVSK. Insofern muss eine normwidrige Handlung im Sinne der Prävention nicht *per se* eine Straftat darstellen. Für die polizeilichen Anwendungsfälle siehe *Seyhan/Eryılmaz*, LD 2004, 7, 25 ff. Anderer Ansicht ist jedoch *Özbek*, DEÜHFD 2002, 86. Nach ihm umfasst das Vorbeugen im Voraus die präemptive Informationssammlung im Vorfeld von Straftaten nicht.

[56] § 7 Abs. 1 lit. b des JTGYK.

[57] Siehe Zusatzparagraph 7 Abs. 1 des PVSK; Zusatzparagraph 5 Abs. 1 des JTGYK.

[58] Die genannten Befugnisse stehen nach § 25 Abs. 1 PVSK auch der Gendarmerie zu.

[59] § 4/A des PVSK.

[60] § 9 Abs. 1 PVSK.

[61] § 13 Abs. 1 PVSK.

von Fingerabdrücken und das Speichern von Personenbildern.[62] Gleichzeitig sind die Polizei und Gendarmerie repressiv tätig, wenn sie als Hilfsorgane der Staatsanwaltschaft Ermittlungen nach der türkischen Strafprozessordnung (tStPO) durchführen (§ 161 Abs. 1 tStPO). Auch hier dürfen sie auf einen breiten Katalog von einzelnen Maßnahmen zurückgreifen, wobei die tStPO beim Treffen prozessualer Maßnahmen durch die Polizei oder Gendarmerie stets vorschreibt, dass entweder im Voraus oder im Nachhinein die Genehmigung bzw. Zustimmung des zuständigen Staatsanwalts (§ 161 Abs. 2 tStPO) einzuholen ist.[63]

Allerdings wäre es ein voreiliger Schluss, anzunehmen, dass die obengenannten präventiven oder repressiven Befugnisse der Polizeibehörden (kolluk) auch der EIDB und dem JIB zustehen, weil die Prävention im türkischen Polizeirecht im weiteren Sinne auch die nachrichtendienstliche Informationssammlung umfasst und diese Dienste nicht nur organisatorisch innerhalb der Polizei bzw. Gendarmerie angesiedelt sind, sondern auch deren Personal Angehörige der Polizei und der Gendarmerie sind. Denn trotz der genannten Zusammenhänge kennt das türkische Polizeirecht eine funktionale Aufgabenaufteilung innerhalb der Polizei und Gendarmerie. Gleichwohl muss man eingestehen, dass sich die Trennung von drei unterschiedlichen Aufgaben (nachrichtendienstliche, gefahrenabwehrende und repressive Tätigkeiten) für die Angehörigen ein und derselben Behörde wohl nicht immer klar vornehmen lässt. Dies öffnet nicht nur Tür und Tor für ein gewisses forum shopping innerhalb der Behörde, wenn bestimmte Maßnahmen ergriffen werden sollen, sondern führt auch dazu, dass die Erfüllung einiger Funktionen zu Gunsten anderer vernachlässigt werden. Dies kann bei der EIDB und beim JIB nicht zuletzt dadurch geschehen, dass diese Dienste eine grundsätzlich auf Strafverfolgung zugeschnittene Informationssammlung betreiben und auch aktiv in die Strafverfolgung herangezogen werden.

Bei näherem Hinsehen lässt sich außerdem konstatieren, dass dem türkischen Inlandsnachrichtendienstrecht insgesamt ein geschlossenes und in sich schlüssiges Konzept über die Auf(gaben)stellung der Dienste fehlt.

d) Unklarheiten im türkischen Inlandsnachrichtendienstrecht

Im türkischen Inlandsnachrichtendienstrecht ist ungeklärt, wer bzw. was die Zielsubjekte oder -objekte der nachrichtendienstlichen Informationssammlung sind. Ob der Gegenstand der nachrichtendienstlichen Tätigkeiten der EIDB etwa bestimmte politische Bestrebungen gegen die obengenannten Rechtsgüter oder darüber hinaus etwa alle Arten der Kriminalität sind, ist im Gesetz nicht geregelt. Auch stellt

---

[62] § 5 Abs. 1 des PVSK. Die genannten Befugnisse stehen nach § 25 Abs. 1 PVSK auch der Gendarmerie. Hierfür siehe auch *Pınarbaşı*, Özel Hayatın Korunması Kapsamında İstihbarat Faaliyetlerinin Hukuksal Sınırları, S. 92.

[63] Hierzu mehr *Arslan*, Einführung und Übersetzung, S. 16 f.

sich die Frage, was unter den nachrichtendienstlichen Tätigkeiten der beiden Behörden gemeint ist. Ob dadurch über die Informationssammlung sowie Beobachtung hinaus weitere Vorgehensweisen gemeint sind, lässt sich aus dem Gesetz nicht ohne Weiteres entnehmen.

Darüber hinaus stellt sich die Frage, was der Zweck der nachrichtendienstlichen Tätigkeiten der EIDB und des JIB ist. Eine ausdrückliche Beschränkung auf die Beratung von politischen Entscheidungsträgern ist nicht ersichtlich. Jedoch macht das Polizeigesetz klar, dass der Zweck der Informationssammlung darin besteht, Vorkehrungen und Schutzmaßnahmen hinsichtlich der obengenannten hochrangigen Güter des Inlandnachrichtendienstrechts zu treffen. Und auch weist das Gesetz als Adressat der gesammelten Informationen auf die zuständigen Instanzen (yetkili merciler) hin.[64] Allerdings lassen diese Einschränkungen nicht den Schluss zu, dass der Zweck der nachrichtendienstlichen Tätigkeiten der EIDB und des JIB lediglich die Beratung von politischen Entscheidungsträgern ist. In der Tat ist nicht nur der Begriff zuständiger Instanzen weit, sondern auch sieht das Gesetz ausdrücklich vor, dass die Informationen an deren „Verwendungsbereich" (kullanma alanına) weiterzuleiten sind,[65] der alles andere als geklärt ist. Zwar liegt es nahe, zu argumentieren, dass der „Verwendungsbereich" nur einer ist, nämlich die nachrichtendienstliche Prävention, zumal das Gesetz vom Bereich im Singular spricht. Allerdings muss die Frage geklärt werden, ob nicht auch die polizeiliche Gefahrenabwehr im Einzelfall sowie die Strafverfolgung diesem Bereich unterfällt.

In der Tat kann das Argument der Singularität spätestens dadurch überwunden werden, dass die Prävention im Sinne des Polizeirechts, wie bereits oben erwähnt, nicht nur die nachrichtendienstliche Nutzung der Informationen, sondern auch die polizeiliche Nutzung im Einzelfall als Gefahrenabwehr umfasst.[66] Außerdem ist darauf hinzuweisen, dass die präventiv-nachrichtendienstliche TKÜ des JIB zum Zwecke der Vorbeugung bestimmter schwerer Katalogstraftaten (suçların işlenmesinin önlenmesi amacıyla) durchgeführt werden darf,[67] und das Polizeigesetz die Durchführung der präventiv-nachrichtendienstlichen TKÜ und der Observation durch die EIDB, ähnlich, nur zum Zwecke der Vorbeugung bestimmter schwerer Katalogstraftaten und Cyberstraftaten (bilişim suçları) zulässt.[68] Vor dem Hintergrund der weitverstandenen Prävention und der Schutzrichtung einiger Maßnahmen der Inlandsdienste ist erneut darauf hinzuweisen, dass der Zweck der nachrichtendienstlichen Tätigkeiten der EIDB und des JIB auch die Gefahrenabwehr im Einzelfall einschließlich der Vorbeugung von Straftaten ist. Insofern lässt sich argumentieren, dass

---

64 Zusatzparagraph 7 Abs. 1 des PVSK.

65 Zusatzparagraph 7 Abs. 1 des PVSK.

66 Vgl. *Yenisey*, Kolluk Hukuku, 129.

67 Zusatzparagraph 5 Abs. 1 des JTGYK.

68 Zusatzparagraph 7 Abs. 2 und Abs. 6 des PVSK; hierzu siehe auch unten I.B.1. MIT, EIDB und JIB.

die polizeiliche Gefahrenabwehr im Einzelfall zu dem „Verwendungsbereich" nachrichtendienstlicher Informationen gehört. Die Vorstellung, dass diese beiden Bereiche voneinander zu trennen sind, herrscht jedenfalls auf dieser Ebene nicht. Dagegen kennen das türkische Inlandsnachrichtendienstrecht sowie das Recht des MIT eine gewisse Trennung zwischen den nachrichtendienstlichen Tätigkeiten und der Strafverfolgung. Daher ist zu klären, ob und inwieweit die Strafverfolgung einen „Verwendungsbereich" darstellt. Um den Umfang der genannten Trennung zu bestimmen, ist zunächst erforderlich, sich die Überschneidungen der Tätigkeiten der Dienste und der Strafverfolgung erneut vor Augen zu führen.

B. Strafverfolgungsrelevante Aufgabenfelder der Nachrichtendienste

1. MIT, EIDB und JIB

Strafverfolgungsrelevante Aufgabenfelder des Nationalen Nachrichtendienstes (MIT) betreffen Spionagestraftaten einschließlich des Schutzes von Staatsgeheimnissen, Terrorismus, internationale Straftaten und Cyberstraftaten.[69] Grundsätzlich ist der MIT auch in diesen Bereichen nachrichtendienstlich, nämlich durch Informationssammlung und Generierung von Erkenntnissen zum Zwecke der Entwicklung einer nationalen Sicherheitspolitik tätig. Dabei fallen auch strafverfolgungsrelevante Informationen an. Dasselbe gilt für die Informationssammlung durch die Inlandsnachrichtendienste (EIDB und JIB). Wie bereits erwähnt, ist die EIDB nicht nur damit beauftragt und befugt, zum Zwecke des Staats-, Verfassungs- und Geheimnisschutzes (Spionage ausgenommen) Informationen zu sammeln, sondern auch die Überwachung des Telekommunikationsverkehrs hinsichtlich schwerer Straftaten des türkischen Strafgesetzbuchs, namentlich einzelne Betäubungsmitteldelikte, Geldwäsche, organisierte Kriminalität zum Zwecke der Erlangung illegalen Profits, Cyberstraftaten, Straftaten gegen die Staatssicherheit, gegen die Verfassungsordnung und deren Funktionieren, die nationale Verteidigung und der Schutz von Staatsgeheimnissen.[70] Die Telekommunikationsüberwachung des JIB erfolgt abgesehen von Cyberstraftaten ebenfalls zur Verhütung der genannten Straftaten.[71]

2. MASAK

Die Kommission zur Ermittlung von Finanzkriminalität (MASAK) vereint in einer besonderen Weise nachrichtendienstlichen Tätigkeiten, polizeiliche Gefahrenabwehr im Einzelfall und Strafverfolgung. Ihre Aufgaben und Befugnisse wurden

---

[69] § 4 Abs. 1 lit. g, h, i des MIT-Gesetzes.

[70] Siehe Zusatzparagraph 7 Abs. 1 und 2 des PVSK.

[71] Zusatzparagraph 5 Abs. 1 des JTGYK.

durch das Präsidialdekret Nr. 1 neu gefasst.[72] Danach beugt die MASAK nicht nur der Terrorismusfinanzierung und der Geldwäsche im Einzelfall vor, sondern generiert nachrichtendienstliche Informationen (istihbarat üretmek).[73] Zu diesen Zwecken sammelt und analysiert sie Finanzinformationen.[74] Diese erhält sie erstens von den meldepflichtigen Personen, die im Gesetz genannt sind.[75] Diese sind verpflichtet, die Transaktionen, bei denen der Verdacht eines illegalen Erwerbs bzw. einer illegalen Verwendung besteht, an die MASAK zu melden.[76] Feststeht, dass der Verdacht im Sinne des MASAK-Gesetzes über den Anfangsverdacht nach der türkischen Strafprozessordnung (tStPO) hinausgeht, zumal sich der erste insgesamt auf Vermögenswerte, die gesetzeswidrig erlangt oder zu gesetzwidrigen Zwecken eingesetzt werden,[77] bezieht, während der Anfangsverdacht der tStPO die Begehung einer Straftat betrifft, die zumindest das Versuchsstadium erreichte.[78] Zweitens ist die Behörde befugt, von sich aus von allen öffentlichen Körperschaften und Anstalten, natürlichen und juristischen Personen sowie Verbänden ohne Rechtspersönlichkeit die Übermittlung von Informationen und die Herausgabe von Dokumenten zu verlangen. Diese sind zur Mitwirkung verpflichtet.[79] Drittens ist die MASAK befugt, andere Verwaltungseinheiten einschließlich der Polizeibehörden zu ersuchen, bestimmte Untersuchungen und Ermittlungen vorzunehmen.[80] Viertens kooperiert sie mit anderen Nachrichtendiensten und den Polizeibehörden und tauscht Informationen aus.[81]

Das strafprozessuale Tätigwerden der MASAK erfolgt zum einen dadurch, dass sie einen Sachverhalt an die zuständige Staatsanwaltschaft übermittelt, wenn sie bei ihren allgemeinen Recherchen auf ernsthafte Verdachtsmomente dahingehend gestoßen ist, dass eine Tat der Geldwäsche oder der Terrorismusfinanzierung begangen

---

[72] Amtsblatt vom 10.07.2018, Nr. 30474. Zuvor wurde § 19 des MASAK-Gesetzes durch das Ausnahmezustandsdekret vom 2.7.2018, Nr. 703 gestrichen. Diese Vorschrift enthielt Bestimmungen über die Aufgaben und Befugnisse der MASAK. Nachdem die gesetzlichen Bestimmungen aufgehoben wurden, war der verfassungsrechtliche Weg frei, diesen Bereich durch ein Präsidialdekret zu regeln (Art. 104 Abs. 17 tVerf.).

[73] § 231 Abs. 1 lit. ç des Präsidialdekrets Nr. 1; siehe auch §§ 17, 18, 19/A des Gesetzes über die Vorbeugung der Verschleierung der Gewinne aus den Straftaten vom 11.10.2006, Nr. 5549, Amtsblatt vom 18.10.2006, Nr. 26323 (abgekürzt: MASAK-Gesetz).

[74] Vgl. §§ 4, 6, 7, 19/A MASAK-Gesetz. Der gleichbedeutende Paragraph § 19 Abs. 1 lit. e und § 21 ist durch § 15 des Dekrets vom 2.7.2018, Nr. 703 gestrichen.

[75] § 2 Abs. 1 lit. d MASAK-Gesetz.

[76] § 4 Abs. 1 MASAK-Gesetz.

[77] § 4 Abs. 1 MASAK-Gesetz.

[78] *Özbek et al.,* Ceza Muhakemesi Hukuku, S. 188–189.

[79] § 7 Abs. 1 und 2 MASAK-Gesetz; siehe auch § 231 Abs. 1 lit. m des Präsidialdekrets Nr. 1.

[80] § 231 Abs. 1 lit. ğ des Präsidialdekrets Nr. 1.

[81] § 231 Abs. 1 lit. h des Präsidialdekrets Nr. 1.

wurde.[82] Zum anderen kann die MASAK in einem Einzelfall nach der Verdachtsmeldung aufgrund der Analyse des Falles Tatsachen feststellen, die auf die Begehung von Geldwäsche oder Terrorismusfinanzierung hinweisen, und bei der Staatsanwaltschaft Anzeige erstatten.[83] Schließlich ist die Behörde als amtliche Sachverständige tätig, wenn es um die Feststellung von Geldwäscheaktivitäten geht und sie zu diesem Zweck von der Staatsanwaltschaft angefragt wird. In solchen Fällen sieht die MASAK die übersandten Akten ein und fertigt ein Gutachten an.[84]

Wie oben angeführt, bestehen nicht nur zwischen den Aufgabenfeldern der MASAK, sondern auch zwischen denen des MIT, der EIDB, des JIB, der MASAK und der Strafverfolgung einige wichtige Überschneidungen. Auf die Frage, was dies im Einzelnen bedeutet und ob und wie das türkische Recht diese beantwortet, wird im Folgenden eingegangen.

II. Interaktion zwischen Nachrichtendiensten und Strafverfolgung

Wie oben bereits betont, besteht organisatorisch eine Trennung zwischen den Nachrichtendiensten und der gefahrenabwehrenden und repressiv tätigen Polizei und Gendarmerie nur hinsichtlich des MITs. Allerdings würde die funktionale und organisatorische Trennung zwischen dem MIT und den anderen Sicherheitsbehörden eindeutig durchbrochen werden, wenn er nun nach der Einführung einzelner neuer operativer Aufgaben auf entsprechende exekutive Befugnisse zurückgreifen würde, deren Ausübung mit der Anwendung unmittelbaren Zwangs einhergehen.[85] Unserer Ansicht nach wäre dies nach der derzeitigen Rechtslage unzulässig.

Die polizeibehördlichen Nachrichtendienste (EIDB und JIB) sind organisatorisch innerhalb der Polizei und Gendarmerie angesiedelt. Organisatorisch sind damit die türkischen Inlandsnachrichtendienste (EIDB und JIB) insofern mit anderen Einheiten der Polizei und Gendarmerie eng verbunden, die die polizeibehördliche Gefahrenabwehr im Einzelfall oder auch die Strafverfolgung betreiben.[86] Im Polizei- und Gendarmeriegesetz sind die beiden Dienste jedoch nach ihrem Aufgabenbereich und Befugnisnormen definiert. Eine funktionale Trennung ist deshalb für die beiden Inlandsdienste anerkannt.

---

[82] § 231 Abs. 1 lit. e des Präsidialdekrets Nr. 1.

[83] § 231 Abs. 1 lit. f des Präsidialdekrets Nr. 1.

[84] § 231 Abs. 1 lit. g des Präsidialdekrets Nr. 1.

[85] Hierzu siehe oben I.A.1b) Befugnisse des MIT.

[86] Vgl. § 9 des Gesetzes über die Organisation der Polizei mit der Nr. 3201, Amtsblatt vom 12.06.1937, Nr. 3629.

Die organisatorische Nähe führt auch personell zu einem engen Verhältnis zwischen der EIDB, dem JIB und der Strafverfolgung, die die Polizeibehörden entsprechend den Weisungen der Staatsanwaltschaft betreiben.[87] Jedoch ist mit der Strafverfolgung grundsätzlich eine getrennte Einheit innerhalb der Polizei, nämlich die Kriminalpolizei (adli kolluk) beauftragt, und nur die Beamten der Kriminalpolizei sind mit den strafverfolgungsrelevanten Aufgaben zu betrauen und auch verpflichtet, von sich aus Anhaltspunkten bezüglich der Begehung von Straftaten nachzugehen (Erstzugriffsrecht).[88] Allerdings sind auch Beamte aus anderen polizeibehördlichen Einheiten der Prävention (önleyici-idari) einschließlich der Beamten der nachrichtendienstlich tätigen Polizei und Gendarmerie verpflichtet und auch berechtigt, das genannte Erstzugriffsrecht auszuüben.[89]

Trotz dieser personellen und organisatorischen Nähe zwischen der EIDB, dem JIB und der Strafverfolgung scheint das türkische Inlandsnachrichtendienstrecht die Probleme, die sich daraus ergeben können, zu anzuerkennen. Diese betreffen nicht zuletzt die Gefahr, dass die Garantien der türkischen Strafprozessordnung hinsichtlich der Ermittlungsmaßnahmen durch einen Rückgriff auf die parallelen nachrichtendienstlichen Maßnahmen umgegangen werden könnten. Damit hängt auch die Verwendung nachrichtendienstlich erlangter Informationen im Strafverfahren eng zusammen. Diese Probleme schneidet das türkische Inlandsnachrichtendienstrecht jedoch nur begrenzt an, wenn in der Begründung des Änderungsgesetzes von 2005 darauf aufmerksam gemacht wird, dass die Befugnis zur nachrichtendienstlichen und präventiven Telekommunikationsüberwachung aufgrund von Bedenken bezüglich möglicher Gefahren nicht allen Einheiten erteilt, sondern nur auf die einzelnen Einheiten in der Polizei (EIDB) und Gendarmerie (JIB) beschränkt wurde.[90] Außerdem wird in der Begründung die Pflicht der beiden Inlandsdienste hervorgehoben, die nachrichtendienstliche Telekommunikationsüberwachung zu beenden und darüber die Staatsanwaltschaft zu benachrichtigen, wenn konkrete Anhaltspunkte vorliegen, die auf die Begehung einer Straftat hinweisen.[91]

Dennoch bedarf der Informationsfluss zwischen den türkischen Nachrichtendiensten (MIT, EIDB und JIB) und der Strafverfolgung näherer Erörterung, um deren Verhältnis zueinander zu veranschaulichen. Dies wird im Folgenden in Zusammenschau mit dem türkischen Strafprozessrecht vorgenommen.

---

[87] § 161 Abs. 2 tStPO; siehe die Vorschrift im Anhnag Gesetezsestexte.

[88] Siehe Zusatzparagraph 6 Abs. 3 des PVSK; vgl. §§ 160 Abs. 1, 161 Abs. 2 tStPO.

[89] Vgl. § 12 Abs. 1 und 2 des Gesetzes über die Organisation der Polizei mit der Nr. 3201, Amtsblatt vom 12.06.1937, Nr. 3629.

[90] Gesetzesbegründung Nr. 924 v. 21.06.2005, S. 8 und 9.

[91] Gesetzsbegründung Nr. 924 v. 21.06.2005, S. 9; für die Heranziehung der in der Begründung aufgestellten Vorgaben des Obersten Strafsenats des Revisionsgerichts, siehe YCGK v. 21.10.2014, E. 2012/4-1283, K. 2014/430.

III. Nachrichtendienstliche Informationen im Strafverfahren

A. Im Allgemeinen

Die Übermittlung von Informationen durch die türkischen Nachrichtendienste (MIT, EIDB und JIB) an die Strafverfolgungsbehörden ist in den Gesetzen der genannten Behörden nur fragmentarisch geregelt, teils als ein ausdrückliches Gebot und teils als Verbot (dazu gleich). In der türkischen Strafprozessordnung hingegen sind keine ausdrücklichen Regelungen vorhanden, weder bezüglich der Übermittlung noch der Verwertung nachrichtendienstlicher Informationen im Ermittlungs- und Hauptverfahren (dazu gleich). Allerdings dürfen diese Umstände nicht darüber hinwegtäuschen, dass in der Praxis in einigen Bereichen ein durchaus reger Informationsfluss von den Diensten an die Strafverfolgung stattfindet und die Strafverfolgungsbehörden sowie die Gerichte von diesen Informationen auch ausgiebig Gebrauch machen. Als rechtliche Grundlage greift man auf die gesetzlichen Generalklauseln zurück. Dennoch sind viele Fragen ungeklärt und das türkische Übermittlungs- sowie das strafprozessuale Beweisrecht ist unter vielen Gesichtspunkten regelungsbedürftig.

B. Übermittlung nachrichtendienstlicher Informationen

1. Übermittlung durch den MIT

a) Selbständige Übermittlung

Das MIT-Gesetz enthält keine Pflicht der Behörde, von sich aus Informationen an die Strafverfolgungsbehörden zu übermitteln. Unklar ist, ob eine solche Pflicht aus den §§ 278, 279 des türkischen Strafgesetzbuchs (tStGB) zu entnehmen ist, welche die Nichtanzeige einer Straftat, die gerade begangen wird oder bereits begangen wurde, unter Strafe stellen.[92]

Allerdings bedeuten die fehlende ausdrückliche Pflicht sowie die Unklarheiten bei der Auslegung des tStGB nicht, dass der MIT von sich aus keine Informationen an die Strafverfolgungsbehörden weiterleiten darf und auch nicht weiterleitet. Im

---

[92] Nichtanzeige einer Straftat (§ 278): (1) Wer eine Straftat, die gerade begangen wird, nicht den zuständigen Behören meldet, wird mit bis zu einem Jahr Gefängnis bestraft.

Nichtanzeige durch einen Amtsträger (§ 279): (1) Der Amtsträger, der im Zusammenhang mit seiner Tätigkeit von einem Offizialdelikt erfährt und es unterlässt oder verzögert, dies den zuständigen Behörden zu melden, wird mit sechs Monaten bis zu zwei Jahren Gefängnis bestraft.

Vgl. zur deutschen Übersetzung *Tellenbach*, Das türkische Strafgesetzbuch, S. 177–178.

Gegenteil räumt die gesetzliche Lücke im Ergebnis dem MIT grundsätzlich einen beachtlichen Ermessensspielraum ein.[93]

In der Tat agiert der MIT genau nach diesem Prinzip, wenn es zu spontanen Übermittlungen kommt. Bekanntestes Beispiel aus jüngerer Zeit sind Informationsübermittlungen an die Staatsanwaltschaft bezüglich der FETÖ/PDY[94]-Fälle, die unter anderem Vorwürfe hinsichtlich des gescheiterten Staatsstreichs am 15. Juli 2016 und Delikte der Bildung einer terroristischen Organisation betreffen. Der MIT veröffentlichte eine Pressemitteilung, in der er ausdrücklich anführte, dass er die Justizinstanzen über die Informationen in Kenntnis setzte, die er bei nachrichtendienstlichen Tätigkeiten erlangt hat. Der MIT gelangte nämlich an Benutzerdaten der MessengerApp „ByLock", die FETÖ/PDY-Mitglieder benutzt haben sollen.[95] Anzumerken ist, dass die Informationsübermittlung durch den MIT an die Strafverfolgungsbehörden nicht auf Staatsschutz- oder Terrorismusdelikte begrenzt ist. Es steht im Ermessen des MITs, die betreffende Straftat für erheblich zu erachten und die diesbezüglichen Informationen weiterzuleiten oder auch nicht. Ebenso wenig ist das Ermessen der Behörde dahingehend beschränkt, Informationen erst beim Erreichen eines bestimmten Verdachtsgrads den Strafverfolgungsbehörden zukommen zu lassen. Somit kann die Behörde Informationen sowohl mit der Kriminalpolizei bzw. Staatsanwaltschaft[96] als auch mit den Strafgerichten[97] teilen.

Das Ermessen des MITs scheint auf den ersten Blick durch den § 6 Abs. 6 des MIT-Gesetzes eingeschränkt zu sein, wonach die Verwendung der nach dem § 6 des MIT-Gesetzes erlangten „Aufnahmen" (kayıtlar) außer zu den in diesem Gesetz genannten Zwecken verboten ist. Hierunter fallen unter anderem „Aufnahmen", die in

---

[93] Das türkische Recht kennt kein verfassungsrechtlich garantiertes Recht auf die informationelle Selbstbestimmung dahingehend, dass die Übermittlung personenbezogener Daten durch den MIT einen Grundrechtseingriff darstellt, der stets einer gesetzlichen Grundlage bedarf. Ob und ggf. inwieweit das verfassungsrechtlich garantierte Recht auf den Schutz von personenbezogenen Daten nach Art. 20 Abs. 3 tVerf in disem Zusammenhang anwendbar ist und für die Rechtmäßigkeit der genannten Übermittlungen eine gesetzliche Grundlage voraussetzt, ist ungeklärt. Dabei enthält das MIT-Gesetz viele Vorschriften über die Geheimhaltung der der Behörde vorliegenden Informationen, etwa § 12 Abs. 1 zu Identitäten der MIT-Beschäftigten, § 29 Abs. 1 bezgl. von Staats- und Dienstgeheimnissen oder auch Zusatzparagraph 1 Abs. 3 mit der Bestimmung der Geheimhaltungsstufen. Aus der Zusammenschau dieser Vorschriften lässt sich ableiten, dass die Behörde als Inhaber und Verwahrer ihres Informationsbestandes nicht nur über die Geheimhaltung, sondern auch über die Offenlegung befinden darf. Dies lässt sich außerdem auch aus dem § 29 des MIT-Gesetzes entnehmen, wonach die MIT-Angehörigen sowie andere Personen, die für den MIT beauftragt worden waren, für eine Aussage als Zeuge der Genehminung der Behörde bedürfen.

[94] Die Abkürzung FETÖ bezieht sich auf „Gülenistische Terrororganisation" [*Fetullahçı Terör Örgütü*] sowie PDY auf „Parallelstruktierter Staat" [*Paralel Devlet Yapılanması*].

[95] http://www.mit.gov.tr/basin60.html.

[96] Vgl. § 158 Abs. 1 tStPO.

[97] Vgl. § 332 Abs. 1 tStPO.

den oben genannten strategischen,[98] individuellen,[99] Ausland-Ausland-, Ausländer-, und anonymen TKÜs[100] erlangt werden.[101]

Der Umfang sowie die Zielrichtung des genannten Verbots sind jedoch nicht klar. Auffällig ist, dass es sich auf die „Aufnahmen" selbst bezieht, und nicht auf die durch die genannten Maßnahmen erhobenen Informationen.[102] Insofern berührt das Verbot nicht direkt das Ermessen des MITs, nachrichtendienstliche Informationen an die Strafverfolgung zu übermitteln, auch wenn diese durch die genannten Methoden erlangt wurden.

Unklarheit besteht auch, wenn es um den Zusatz „außer den in diesem Gesetz bestimmten Zwecken" geht. Man kann zwar anführen, dass die Informationssammlungen des MITs jedenfalls nicht primär die Förderung der Strafverfolgung bezwecken.[103] Damit würde man in § 6 Abs. 6 des MIT-Gesetzes ein Verwendungsverbot für die „Aufnahmen" der genannten Maßnahmen auch im Strafverfahren sehen. Allerdings stellt sich bei einer genauen Lektüre des MIT-Gesetzes heraus, dass die Förderung der Strafverfolgung diesem Gesetz nicht völlig unbekannt ist. So dürfen etwa die Justizinstanzen einschließlich der Strafgerichte vom MIT in Bezug auf die Straftaten gegen Staatsgeheimnisse und Spionage (§ 326–339 tStGB) Informationen anfordern (hierzu gleich unten).[104] Die Hilfestellung für die Strafverfolgung ist demgemäß, wenn auch sekundär, doch ein im MIT-Gesetz vorgesehener Zweck im Sinne des § 6 Abs. 6.[105] Der Verwendung der „Aufnahmen" im Strafverfahren wegen Straftaten gegen Staatsgeheimnisse und Spionage (§ 326–339 tStGB) steht also § 6 Abs. 6 des MIT-Gesetzes nicht entgegen. Warum dann die „Aufnahmen" auch in anderen Strafverfahren nicht verwendet werden dürfen, ist nicht geklärt.

Es liegt zum einen nahe, dass der Gesetzgeber eine Umgehung der in anderen Gesetzen einschließlich der tStPO vorgesehenen Ermächtigungsgrundlagen vorbeugen wollte.[106] In der Tat besteht weniger Anreiz dafür, den MIT zu ersuchen, Maßnahmen des § 6 MIT-Gesetzes einschließlich der genannten TKÜs zu ergreifen, die unter anderem deutlich niedrigere Ermittlungsschwellen voraussetzen, wenn die ersuchende Behörde von vornherein weiß, dass die erlangten „Aufnahmen" etwa im

---

98 § 6 Abs. 1 lit. g. des MIT-Gesetzes.

99 § 6 Abs. 2 bis 9 des MIT-Gesetzes.

100 § 6 Abs. 10 des MIT-Gesetzes.

101 Hierzu siehe auch oben I.A.1.b) Befugnisse des MIT.

102 Nach einer anderen Literaturansicht verwendet der Gesetzgeber den Begriff „Aufnahmen", weil es sich hier im strengen Sinne nicht um Beweismittel des Strafprozesses handelt, sondern um nachrichtendienstlich relevantes Material, s. *Turhan/Aksu*, KD 2009, 2216; *Birtek*, CHD 2011, 125.

103 Siehe oben I.A.1a) Aufgaben des MIT.

104 Zusatzparagraph 1 Abs. 1 des MIT-Gesetzes.

105 Zuzugeben ist, dass der Verweis des § 6 Abs. 6 des MIT-Gesetzes auf die weiteren Zwecke des Gesetzes eine gewisse Zirkularität aufweist, die sich schwer auflöst.

106 Vgl. *Şahin*, GÜHFD 2007, 1097.

Strafverfahren nicht verwendet werden dürfen. Zum anderen fungiert § 6 Abs. 6 des MIT-Gesetzes als eine Missbrauchsklausel, die eine willkürliche Zweckentfremdung der genannten Aufnahmen, etwa zum Zwecke der politischen oder wirtschaftlichen Einflussnahme, verbietet. Dennoch muss an dieser Stelle erneut betont werden, dass sich das Verbot der Verwendung von „Aufnahmen" nach § 6 Abs. 6 des MIT-Gesetzes nicht allgemein auf Informationen des MIT bezieht, sei es durch die genannten Überwachungsmaßnahmen oder anderweitig. Diese Vorschrift ändert also im Ergebnis an dem Ermessen des MITs, nachrichtendienstliche Informationen an die Strafverfolgung zu übermitteln, nichts.

b) Übermittlung auf Anfrage der Strafverfolgungsbehörden

Die Staatsanwaltschaft darf nach § 161 Abs. 1 tStPO von allen Beamten des öffentlichen Dienstes Auskünfte hinsichtlich einer zu ermittelnden Straftat ersuchen. Nach § 332 Abs. 1 tStPO ist es obligatorisch, unter anderem die Auskunftsersuchen der Staatsanwaltschaft im Ermittlungsverfahren sowie die der Tatgerichte im Hauptverfahren förmlich entgegenzunehmen und zu erfüllen. Beide Vorschriften richten sich grundsätzlich auch an den MIT. Nach §§ 125 Abs. 1, 47 Abs. 1 tStPO darf die Erfüllung strafgerichtlicher Auskunftsersuchen sogar auch dann nicht verweigert werden, wenn es sich bei den in Frage stehenden Informationen um Staatsgeheimnisse handelt. Diese müssen durch ein sogenanntes In-camera-Verfahren ins Hauptverfahren eingeführt werden.[107] Auch diese Vorschriften gelten grundsätzlich für den MIT. Allerdings hat eine Gesetzesänderung im Jahre 2014 eine Ausnahme von diesen Verpflichtungen nach §§ 161 Abs. 1, 332 Abs. 1 tStPO und der Durchführung des In-camera-Verfahrens nach §§ 125 Abs. 2, 47 Abs. 2 tStPO vorgesehen. Nach dem Zusatzparagraph 1 des MIT-Gesetzes dürfen die Justizorgane vom MIT nicht anfordern, Informationen, Schriftstücke, Angaben oder Eintragungen und Analysen herauszugeben, wenn diese durch den MIT als nachrichtendienstliche Informationen eingestuft sind. Damit ist der MIT zum einen grundsätzlich von den Auskunftserfüllungspflichten nach §§ 161 Abs. 1, 332 Abs. 1 tStPO befreit. Zum anderen muss der MIT die in Frage stehenden Informationen nicht mehr nach §§ 125 Abs. 2, 47 Abs. 2 tStPO durch ein In-camera-Verfahren ins Hauptverfahren einführen, wenn diese Staatsgeheimnisse darstellen. Denn das Anforderungsverbot hat zur Folge, dass gar keine Pflicht für den MIT entsteht, nachrichtendienstliche Informationen zu übermitteln, die dann durch das In-camera-Verfahren zu schützen wären, wenn diese gleichzeitig Staatsgeheimnisse sind. Von dem Anforderungsverbot macht jedoch der Zusatzparagraph 1 des MIT-Gesetzes eine Ausnahme, wenn die nachrichtendienstlichen Informationen Straftaten gegen Staatsgeheimnisse und Spionage (§§ 326 ff. tStGB) betreffen.

---

[107] Hierzu mehr siehe *Arslan*, Staatsgeheimnisse, S. 22 f.

Bei näherem Hinsehen lässt sich feststellen, dass das Anforderungsverbot Anfragen oder Anregungen seitens der Justizinstanzen für eine Informationsübermittlung nicht untersagt. Denn es besagt lediglich, dass eine für den MIT rechtsverbindliche Informationsanfrage, wie in §§ 161 Abs. 1, 332 Abs. 1 tStPO vorsehen, nicht gestellt werden darf bzw. der MIT daran nicht gebunden ist. Die Stellung rechtsunverbindlicher Anfragen ist damit nicht ausgeschlossen. Eine solche würde etwa vorliegen, wenn es um Auskunftsermittlungsanfragen der Staatsanwaltschaft oder der Gerichte geht, die nicht die Straftaten gegen Staatsgeheimnisse und Spionage (§§ 326 ff. tStGB) betreffen. Dies lässt sich für den MIT als eine bloße Anregung verstehen, die freilich weder §§ 161 Abs. 1, 332 Abs. 1 tStPO aktivieren noch eine förmliche Bearbeitung seitens des MIT veranlassen kann. Insofern ist darauf hinzuweisen, dass das obengenannte allgemeine Ermessen des MITs auch hier gilt. Es steht außer Frage, dass stichhaltige Darstellungen der Staatsanwaltschaft sowie der Strafgerichte den MIT zu einer Informationsübermittlung ermutigen würden. Die Frage, ob etwa die Staatsanwaltschaft den MIT ersuchen kann, nicht nur aus dem vorhandenen Informationsbestand nach einschlägigen Informationen zu suchen, sondern sich auf die Suche nach neuen Informationen zu machen, ist im MIT-Gesetz nicht beantwortet.

Außerdem bedeutet das genannte Anforderungsverbot nicht, dass der MIT außer den genannten Straftaten keinerlei Informationen an die Justizorgane übermitteln darf oder übermittelt. Wie bereits oben hinsichtlich der spontanen Übermittlungen festgestellt, steht es im Ermessen des MITs, die in der Auskunftsermittlung genannte Straftat für erheblich zu erachten und die diesbezüglichen Informationen zu übermitteln. Des Weiteren heißt die Stellung einer Anfrage bezüglich der Straftaten gegen Staatsgeheimnisse und Spionage nicht, dass der MIT zur Informationsübermittlung uneingeschränkt verpflichtet ist.

c) Zurückhaltung von nachrichtendienstlichen Informationen durch den MIT

aa) Bei der Erteilung einer Aussagegenehmigung

Wie bereits mehrfach betont, genießt der MIT einen weitestgehenden Ermessensspielraum, darüber zu entscheiden, ob er nachrichtendienstliche Informationen von sich aus oder auf Anfrage an die Strafverfolgungsbehörden übermittelt, sowie bei welchem Verdachtsgrad und hinsichtlich welcher Straftaten. Auch nennt das MIT-Gesetz selbst sehr wenige Gründe, auf die sich der MIT berufen kann, wenn er sich für die Nichtübermittlung entscheidet.

In seiner ersten Fassung verlangte § 29 des MIT-Gesetzes eine Genehmigung des Präsidenten des MIT, wenn die Angehörigen des MIT als Zeuge angehört werden sollten und dies ein Dienstgeheimnis oder staatliche Interessen betraf. Fehlte ein solcher Bezug, so galt die allgemeine strafprozessuale Aussagepflicht auch für die Angehörigen des MIT. Der Präsident des MIT durfte die Aussagegenehmigung erteilen oder verweigern, je nachdem, welche Entscheidung im konkreten Fall für den Schutz

der Dienstgeheimnisse oder der staatlichen Interessen erforderlich war.[108] Während der Schutz von Dienst- oder Staatsgeheimnissen in der Regel für eine Verweigerung der Aussagegenehmigung sprachen,[109] durfte der Präsident des MIT die Aussagegenehmigung trotzdem erteilen, wenn dies für die Wahrung anderer staatlicher Interessen, etwa der Strafgerechtigkeit, erforderlich war. Allerdings sah die Praxis eher so aus, dass man in aller Regel die Aussagegenehmigung zum Schutz von anderweitigen amtlichen Interessen völlig verweigerte (Sperrung) und staatliche Interessen wie die Gewährleistung der Strafjustiz kaum berücksichtigte.[110]

Im Jahr 2005 änderte die neue türkische Strafprozessordnung diese Rechtslage völlig. Wie bereits oben erwähnt, erfordern die §§ 47 Abs. 1, 125 Abs. 1 tStPO, dass alle Behörden und Personen einschließlich des MIT und seiner Angehörigen, als Zeuge auszusagen haben und Informationen oder anderweitiges Beweismaterial gegenüber einem Strafgericht durch das sogenannte In-camera-Verfahren offenzulegen haben, wenn diese Staatsgeheimnisse darstellten.[111] Als späteres Gesetz gingen §§ 47 Abs. 1, 125 Abs. 1 tStPO dem § 29 des MIT-Gesetzes vor und der Präsident des MIT durfte damit Zeugen nicht mehr sperren.

Diese Rechtslage hat jedoch nur neun Jahre überlebt und 2014 hat eine Gesetzesänderung für den MIT eine Ausnahme von den strengen Offenlegungspflichten des §§ 47 Abs. 1, 125 Abs. 1 tStPO eingeführt. Danach ist es für die Beamten des Nationalen Nachrichtendienstes sowie jenen, die Aufträge des Nationalen Nachrichtendienstes erfüllt haben (etwa Informanten), untersagt, als Zeuge auszusagen. Die neue Fassung des § 29 MIT-Gesetzes verlangte nicht mehr, dass die Zeugenaussage einen Bezug zu Dienstgeheimnissen oder anderen staatlichen Interessen aufweisen muss. Sie hob die allgemeine strafprozessuale Aussagepflicht für die Angehörigen des MIT schlechthin auf und machte eine Ausnahme dahingehend, dass die MIT-Angehörigen einer Genehmigung des Präsidenten des Dienstes bedürfen und der Präsident selbst die des Ministerpräsidenten bedarf, wenn die Zeugenaussagen zur Wahrung staatlicher Interessen erforderlich sind.[112]

Das türkische Verfassungsgericht erklärte diese Regelung in einer Entscheidung aus dem Jahre 2015 für verfassungswidrig, weil sie für bestimmte Personen die Aussage als Zeuge kraft Gesetzes pauschal verbiete, ohne dass ein Bezug der in Frage

---

[108] So das tVerfGE Urteil v. 30.12.2015 E. 2014/122 K. 2015/123 § 190, Amtsblatt v. 01.03.2016 Nr, 29640.

[109] Ähnlich räumte § 49 Abs. 1 der türkischen Strafprozessordnung von 1929 (in damaliger Fassung) einem Behördenleiter die Befugnis ein, die Aussagegenehmigung für einen Beamten zu verweigern, wenn dieser ansonsten Geheimnisse offenbaren müsste, durch deren Bekanntwerden dem Wohl des Staates Nachteile entstehen würden; näher siehe *Arslan*, Staatsgeheimnisse, S. 16.

[110] Siehe auch *Arslan*, Staatsgeheimnisse, S. 17 ff.

[111] Für mehr siehe *Arslan*, Staatsgeheimnisse, S. 23 ff.

[112] Für den türkischen Text siehe tVerfGE Urteil v. 30.12.2015 E. 2014/122 K. 2015/123 § 6, Amtsblatt v. 01.03.2016 Nr. 29640.

stehenden Aussage zu Aufgaben des MIT vorliegen, der Präsident des MIT über eine Aussagegenehmigung entscheiden und eventuell für die Verweigerung einen stichhaltigen Grund nennen muss. Dadurch erschwert sie nach dem tVerfG nicht nur die Findung der materiellen Wahrheit, die für die Strafgerechtigkeit essentiell ist, sondern auch die Gewährleistung der Verteidigungsrechte. Außerdem berücksichtige die genannte Regelung bei der Erteilung einer Aussagegenehmigung lediglich die Erfordernisse staatlicher Interessen. Diese können dahingehend verstanden werden, dass individuelle Interessen nicht berücksichtigt zu werden brauchen.[113]

Der türkische Gesetzgeber reagierte auf die Entscheidung des tVerfG und fasste § 29 des MIT-Gesetzes 2017 neu. Dabei hat er die oben aufgeführte ursprüngliche Fassung beinahe wortgleich erneut eingeführt. Insofern sind die MIT-Angehörigen sowie jene Personen, die Aufträge für den MIT erfüllt haben, im Strafprozess grundsätzlich aussagepflichtig. Weist jedoch die in Frage stehende Aussage einen Bezug zu einem Dienstgeheimnis oder anderen staatlichen Interessen auf, so hat der Präsident des MIT eine Entscheidung zu treffen, ob deren Schutz die Verweigerung der Aussagegenehmigung erfordert. Zwar zählt auch die Gewährleistung der Strafgerechtigkeit zu den staatlichen Interessen, allerdings legt schon die oben erwähnte alte Praxis des § 29 des MIT-Gesetzes die Vermutung nahe, dass diese in der Regel den Geheimhaltungsinteressen des Dienstes und anderweitigen staatlichen Interessen wohl nachgeordnet wird.[114]

bb) Ermessen des MIT in anderen Fällen und die Würdigung der Entscheidung des tVerfG

Wie bereits oben angeführt, darf der MIT auch bei förmlich zugelassenen Anforderungen oder Anfragen/Anregungen die Herausgabe von Informationen, Schriftstücken, Angaben oder Eintragungen und Analysen an Justizorgane verweigern (Zusatzparagraph 1 des MIT-Gesetzes). Gründe dafür, wie es bei der Verweigerung der Aussagegenehmigung der Fall ist, nennt das MIT-Gesetz nicht.

Trotz der weitreichenden Auswirkungen dieser Vorschrift auf das Strafverfahren, sowohl für das Gericht als auch für die Verteidigung, billigte das türkische Verfassungsgericht (tVerfG) in der bereits oben genannten Entscheidung deren Verfassungsmäßigkeit.

Einerseits betonte das Gericht, dass jede Norm, die die Wahrheitsermittlung erschwert, der Verwirklichung der Gerechtigkeit abträglich ist und dadurch auch gegen

---

[113] Zum türkischen Text siehe tVerfGE Urteil v. 30.12.2015 E. 2014/122 K. 2015/123 §§ 190 ff., Amtsblatt v. 01.03.2016 Nr. 29640.

[114] Schließlich dürfen sich auch die Beamte des MIT sowie andere Personen, die für den MIT arbeiten, etwa Informanten, auf den allgemeinen Zeugenschutz im Strafverfahren berufen. Näher siehe *Arslan*, Staatsgeheimnisse, S. 35 ff.

das Rechtsstaatsprinzip und den Anspruch auf rechtliches Gehör verstößt.[115] Gleichzeitig stellt das tVerfG in einem bemerkenswerten Zug fest, dass die Nichtübermittlung nachrichtendienstlicher Informationen bei Anfragen an die Justizorgane einschließlich des Strafgerichts diesen Tatbestand nicht erfüllt. Denn die nachrichtendienstlichen Informationen seien nicht als Beweis anzusehen und deshalb erschwere die Unkenntnis solcher Informationen die Wahrheitsermittlung nicht! Das tVerfG wies darauf hin, dass die nachrichtendienstlichen Informationen im Wesentlichen nicht „gesichert" (kesin) seien und deshalb keine Beweise darstellten. Außerdem führte es an, dass die Funktionstüchtigkeit des MIT lebenswichtig sei, um die nationale Sicherheitspolitik zu bestimmen, präventive Maßnahmen zu treffen und Maßnahmen der Spionageabwehr durchzuführen. Daher müsse das Ermessen des MIT auch gegenüber den Justizinstanzen gelten. Schließlich machte das tVerfG darauf aufmerksam, dass die angefochtene Gesetzesänderung bezweckt habe, die Aufdeckung nachrichtendienstlicher Informationen während des öffentlichen Verfahrens zu verhindern. Die Verhinderung der Wahrheitsermittlung sei dabei nicht intendiert gewesen.[116]

Die Begründung des tVerfG, dass Geheiminformationen beim Tatvorwurf irrelevant und im Verfahren unanwendbar seien, weil sie nicht „gesichert" seien, ist in keinem Falle überzeugend, da das Gesetz selbst bereits eine Ausnahme macht, nach der eine Anfrage für die Übermittlung nachrichtendienstlicher Information an die Justizorgane bei einigen Straftaten zulässig ist. Das Gericht ließ die Frage offen, warum bei einer möglichen Übermittlung nachrichtendienstliche Information in diesen Fällen als „gesichert" betrachtet werden können und warum in anderen Fällen keineswegs. Freilich zielt das Argument, dass der MIT eine sehr wichtige öffentliche Aufgabe erfüllt und an dem Nichtbekanntwerden seiner Informationen großes Interesse hat, in die richtige Richtung. Es ist aber unbefriedigend, öffentliche Interessen an der Wahrheitsermittlung mit einer vermeintlichen Untauglichkeit nachrichtendienstlicher Informationen abzutun. Stattdessen hätte es sich angeboten, entsprechend dem Verhältnismäßigkeitsgrundsatz einen Ausgleich zwischen den konfligierenden Interessen aufzuzeigen.[117] Der Gesetzgeber selbst scheint den Ausgleich zunächst darin gefunden zu haben, dass eine Anfrage über nachrichtendienstliche Informationen bei Straftaten gegen Staatsgeheimnisse und Spionage (§§ 326 ff. tStGB) zulässig ist. Anstatt eine vermeintliche Untauglichkeit nachrichtendienstlicher Informationen zu postulieren, hätte das tVerfG gut daran getan, sich mit der Verfassungsmäßigkeit des gesetzgeberischen Ausgleiches auseinanderzusetzen. Dabei hätte das Gericht zumindest der Frage nachgehen müssen, aus welchen Gründen

---

[115] tVerfGE Urteil v. 30.12.2015 E. 2014/122 K. 2015/123 § 203, Amtsblatt v. 01.03.2016 Nr. 29640.

[116] tVerfGE Urteil v. 30.12.2015 E. 2014/122 K. 2015/123 § 204 f., Amtsblatt v. 01.03.2016 Nr. 29640.

[117] tVerfGE Urteil v. 30.12.2015 E. 2014/122 K. 2015/123 § 206, Amtsblatt v. 01.03.2016 Nr: 29640.

der MIT auch bei einer zulässigen Anforderung bei Straftaten gegen Staatsgeheimnisse und Spionage (§§ 326 ff. tStGB) die Informationsübermittlung verweigern darf.

In Wirklichkeit billigt das Urteil stillschweigend wiederum das bereits oben mehrfach angesprochene Ermessen des MIT, über alle Anfragen sowie Anregungen hinsichtlich der Informationsübermittlung uneingeschränkt bestimmen zu können. Das Fehlen klarer Ermächtigungsnormen zum Zurückhalten nachrichtendienstlicher Information macht den MIT für Vorwürfe angreifbar, Machtmissbrauch zu betreiben. In der Tat ist es dem türkischen Nachrichtendienstrecht noch nicht gelungen, objektive Kriterien für die Zurückhaltung nachrichtendienstlicher Informationen aufzustellen. Da sich das tVerfG in dem obengenannten Urteil auch die Chance entgehen ließ, darauf zu drängen, ist es derzeit dem Gesetzgeber überlassen, in diesem Sinne tätig zu werden und die bestehenden Gesetzeslücken zu füllen.

2. Übermittlung durch die EIDB und das JIB

Gesetzeslücken sind auch vorhanden, wenn es um die Informationsübermittlungen der EIDB und des JIB, sei es von sich aus oder sei es auf Anfragen, an die Strafverfolgungsbehörden geht. Das Fehlen eines Anforderungsverbots oder der Möglichkeit der Verweigerung der Aussagegenehmigung, wie es das MIT-Gesetz vorsieht, impliziert allerdings, dass die von den beiden Diensten erlangten Informationen im Vergleich zu Beweissammlungen der Strafverfolgung weder für grundverschieden erachtet werden noch sich die beiden Dienste als mit Anfragen oder der Erteilung von Aussagegenehmigungen überfordert ansehen. Außerdem legen die Umstände, dass die Tätigkeiten der EIDB und des JIB im weiteren Sinne als Prävention betrachtet werden, die beiden Dienste im allgemeinen Polizeirecht (kolluk hukuku) geregelt und unter dem „Dach" der allgemeinen Polizeibehörden angesiedelt sind, die Vermutung nahe, dass eine strenge informationelle Trennung zwischen der EIDB und dem JIB nicht intendiert ist. Im Gegenteil scheint es eher der Fall zu sein, dass sich die türkischen Inlandsnachrichtendienste als *law enforcement intelligence* verstehen, worunter auch die Strafverfolgung (crime intelligence) fällt. Dies ist insbesondere für das JIB augenscheinlich, der, wie bereits oben erwähnt, im Gegensatz zur EIDB keinen allgemeinen Aufgabenbereich für die nachrichtendienstlichen Tätigkeiten hat, sondern lediglich mit der Vorbeugung bestimmter schwerer Katalogstraftaten betraut ist. Grundsätzlich scheint es so zu sein, dass die von der Prävention unzureichend abgegrenzten funktionalen Aufgabenbereiche des EIDB und des JIB und die organisatorische und personelle Nähe der beiden Behörden zur Strafverfolgung zu einer gewissen informationellen „Einheit" mit der Strafverfolgung führen.

Gleichzeitig ist sich der türkische Gesetzgeber wohl bewusst, dass dieser eher der konzeptionellen Aufstellung der beiden Dienste geschuldete Zustand Bedenken hervorruft, wenn es um die Übermittlung von Informationen geht, die die EIDB und das JIB durch nachrichtendienstliche Tätigkeiten erlangt haben. Dies zeigen die

gleichlautenden Vorschriften für die beiden Dienste, wonach „die Aufnahmen, die im Rahmen der nach diesem Paragraph geführten Tätigkeiten erlangt werden, außer zu den im ersten Absatz genannten Zwecken nicht verwendet werden dürfen“.[118] Gemeint sind hier Aufnahmen, die unter anderem bei öffentlichen Stellen,[119] durch die Observation mit technischen Mitteln,[120] sowie durch die Überwachung der Telekommunikation[121] und des Datenverkehrs im Internet erlangt wurden.[122] Wie bereits oben erwähnt, sind die zuletzt genannten Überwachungsmaßnahmen nur zulässig, um bestimmten schweren Katalogstraftaten und Cyberstraftaten vorzubeugen.[123] Im Gegensatz zur Vorbeugung fällt damit die Verfolgung von Straftaten nicht unter die Zwecke, für deren Erfüllung die aus diesen Maßnahmen gewonnenen Informationen verwendet werden dürfen.

Allerdings wäre es voreilig, daraus zu schließen, dass die beiden Inlandsdienste entsprechend dem genannten Verwendungsverbot keine Informationen an die Strafverfolgung übermitteln dürfen. Denn wie im MIT-Gesetz bezieht sich auch hier das Verwendungsverbot auf die „Aufnahmen“ (kayıtlar), ein Begriff, dessen Auslegung alles andere als klar ist. Die aus diesen „Aufnahmen“ gewonnenen Informationen fallen wohl nicht darunter. In der Tat entsprechen die Berichte aus der Praxis diesem Bild, wonach etwa die EIDB grundsätzlich auf regulärer Basis nachrichtendienstlich gesammelte Informationen im Fall eines Anfangsverdachts an die jeweiligen repressiv-polizeilichen Einheiten, etwa die Abteilung für die Bekämpfung des Terrorismus oder der organisierten Kriminalität, weiterleitet.[124] Es lässt sich sogar argumentieren, dass die Beamten der EIDB, für die ja das Polizeigesetz und die Strafprozessordnung weiterhin gelten, zur Informationsübermittlung verpflichtet sind. In der Tat spürt der türkische Gesetzgeber kein Bedürfnis, im Inlandsnachrichtendienstrecht die Informationsübermittlung zwischen den Diensten und der Strafverfolgung zu regeln. Er belässt es, wie im MIT-Gesetz, mit dem Verwendungsverbot des Polizei- und Gendarmeriegesetzes bei einem Umgehungs- und Missbrauchsverbot. Die EIDB und das JIB dürfen also von sich aus oder auf Anfrage nachrichtendienstliche Informationen an die Kriminalpolizei, die Staatsanwaltschaft und die Strafgerichte übermitteln, ohne dass sie dafür einen bestimmten Verdachtsgrad bräuchten.

3. Zwischenergebnisse

Im Ergebnis lässt sich feststellen, dass die Übermittlung der nachrichtendienstlichen Informationen in allen Bereichen der Kriminalität nach türkischem

---

118 Zusatzparagraph 7 Abs. 7 des PVSK; Zusatzparagraph 5 Abs. 6 des JTGYK.

119 Siehe Zusatzparagraph 7 Abs. 6 des PVSK; Zusatzparagraph 5 Abs. 5 des JTGYK.

120 Siehe Zusatzparagraph 7 Abs. 6 des PVSK; Zusatzparagraph 5 Abs. 5 des JTGYK.

121 Siehe Zusatzparagraph 7 Abs. 2 des PVSK; Zusatzparagraph 5 Abs. 1 des JTGYK.

122 Siehe Zusatzparagraph 7 Abs. 2 des PVSK.

123 Zusatzparagraph 7 Abs. 2 und Abs. 6 des PVSK.

124 *Özbek*, DEÜHFD 2002, 82; *Kuloğlu*, PBD 2012, 11.

Nachrichtendienstrecht zulässig ist. Auch in der Praxis ist es nicht ungewöhnlich, dass der MIT, die EIDB oder das JIB aus eigenem Antrieb oder auf deren Anfrage oder Anregung der Kriminalpolizei, der Staatsanwaltschaft oder auch den Gerichten Informationen zukommen lassen. Zahlreiche Gerichtsentscheidungen, die ausdrücklich Bezug auf die nachrichtendienstlichen Informationen nehmen, belegen dies.[125] Kennzeichnend für das türkische Übermittlungsrecht ist, dass den Diensten in allen Bereichen ein alleiniger und beachtlicher Ermessensspielraum zusteht. Es kennt zwar einige Verwendungsverbote, deren Umfang ist allerdings nicht nur unklar, sondern auch bei näherem Hinsehen nicht weitreichend. Außerdem enthält lediglich das MIT-Gesetz einzelne Gründe für die Zurückhaltung von Informationen im Falle einer Zeugenaussage. In den übrigen Fällen bleibt die Bestimmung der Zurückhaltungsgründe den Diensten überlassen.

C. Verwendung nachrichtendienstlicher Informationen im Strafverfahren

1. Im Ermittlungsverfahren

Wie bereits oben festgestellt, dürfen alle Nachrichtendienste in der Türkei von sich aus Informationen an die Kriminalpolizei oder die Staatsanwaltschaft übermitteln. Das Erreichen eines bestimmten Verdachtsgrads ist nicht erforderlich.[126] Ebenso darf die Staatsanwaltschaft gemäß § 161 Abs. 1 tStPO „*... von allen öffentlichen Bediensteten jegliche Art von Auskunft verlangen*“.[127] Darunter fallen diese drei Dienste, wobei das MIT-Gesetz die Stellung einer förmlichen Anforderung lediglich auf einen engen Bereich der Straftaten begrenzt. Wie bereits oben erwähnt, ist eine Anregung damit aber nicht verboten.

Die Staatsanwaltschaft kann die übermittelten Informationen für verschiedene Maßnahmen nutzen. Dabei ist sie an die Bewertungen, die in den nachrichtendienstlichen Berichten enthalten sind, nicht gebunden. Sie muss die Richtigkeit, Zuverlässigkeit, Glaubwürdigkeit und den Beweiswert der Information selbst überprüfen.[128] Das türkische Strafprozessrecht kennt keine Norm, die die Verwendung nachrichtendienstlicher Informationen an die Erfüllung bestimmter Voraussetzungen knüpft, damit ein gewisser Grundrechtsschutz der von der Informationsübermittlung

---

[125] Siehe YCGK. Urt. v. 14.02.2012 E. 2011/10-212, K. 2012/42; YCGK. Urt. v. 14.12.2010 E. 2010/9-88, K. 2010/255; YCGK. Urt. v. 15.03.2005 E. 2005/10-15 K. 2005/29; 9. YCD. Entsch. v. 24.10.2005 E. 2005/5497 K. 2005/7945; 10. YCD. Entsch. v. 20.10.2010 E. 2010/25370 K. 2010/22325.

[126] Das Fehlen eines bestimmten Verdachtgrades wird in der Literatur kritisiert und eine detaillierte Regelung wie im deutschen Polizeirecht empfohlen. Siehe *Yenisey*, Kolluk Hukuku, 130.

[127] *Arslan*, Einführung und Übersetzung, S. 177; siehe auch § 332 Abs. 1 tStPO.

[128] *Arslan*, ABD 2013, 62.

betroffenen Personen gewährleistet sowie der Umgehung von strafprozessualen Garantien vorgebeugt werden kann.[129] Basierend auf diesen Informationen kann sie Maßnahmen wie die Vernehmung von Beschuldigten oder von Zeugen, Festnahmen, Durchsuchungen, die Beantragung der Untersuchungshaft oder auch die Überwachung des Telekommunikationsverkehrs einleiten. Da für das Ermittlungsverfahren der Grundsatz der Geheimhaltung gilt (§ 157 Abs. 1 tStPO) und die Staatsanwaltschaft durch einen richterlichen Beschluss bei bestimmten Katalogstraftaten und beim Vorliegen einer Gefährdung des Ermittlungserfolges der Verteidigung den Aktenzugang entziehen kann (§ 153 Abs. 2 tStPO), wird der Verteidigung im Ermittlungsverfahren in der Regel verborgen bleiben, ob und ggf. welche nachrichtendienstlichen Informationen gegen den Beschuldigten verschiedentlich verwendet wurden.[130] Freilich kann sich die Staatsanwaltschaft in der Anklageschrift auf die nachrichtendienstlichen Informationen stützen, die sie grundsätzlich mit der Übergabe der Akten an das Tatgericht diesem und der Verteidigung offenlegen muss (§ 170 Abs. 3 lit. j tStPO). Allerdings impliziert diese Befugnis der Staatsanwaltschaft auch, dass die Staatsanwaltschaft die Verwendung nachrichtendienstlicher Informationen im Ermittlungsverfahren gänzlich geheim halten kann. Dies wird es nicht selten der Verteidigung erschweren, Rechtmäßigkeit und Verlässlichkeit der gegen den Beschuldigten verwendeten Beweismittel anzufechten, und dadurch das Recht des Beschuldigten auf ein faires Verfahren nach Art. 6 Abs. 1 EMRK beeinträchtigen.[131]

2. Im Hauptverfahren

Auch in das Hauptverfahren können nachrichtendienstliche Informationen eingeführt und in diesem genutzt werden.[132] Voraussetzung ist dafür jedoch, dass die Anklage die bereits genannte Offenlegungspflicht erfüllt[133] und/oder das Tatgericht die Herbeischaffung der womöglich zurückgehaltenen nachrichtendienstlichen

---

[129] Beispielsweise ist die unmittelbare Verwendung der nachrichtendienstlichen Informationen von deutschen Strafverfolgungsbehörden einschließlich der Gerichte nur dann möglich, wenn derartige Informationen auch in Übereinstimmung mit der dStPO hätten gesammelt werden können (sogenannter hypothetischer Ersatzeingriff nach § 161 Abs. 2 dStPO).

[130] Dies führt in der Praxis dazu, dass die Verteidigung beim Rechtsschutz gegen die gegen den Beschuldigten verhängten Ermittlungsmaßnahmen kaum Erfolgschancen hat. Vgl. §§ 268–269 tStPO.

[131] Zu den Offenlegungspflichten der Anklagebehörde siehe EGMR Edwards und Lewis ./. Vereinigtes Königreich Urt. v. 22.07.2003 § 58; EGMR Natunen ./. Finnland Urt. v. 31.03.2009 § 47.

[132] Die Zurückhaltung der Identität von Belastungszeugen sowie die Einführung der Zeugenaussagen etwa durch Zeugenschutzmethoden werden hier aus Platzgründen nicht erörtert; hierzu siehe *Arslan*, Staatsgeheimnisse, S. 35 ff. und 54 ff.

[133] Bei der Anklageerhebung kann das Gericht die Anklageschrift unter anderem deswegen zurückweisen, wenn die der Anklage zugrundeliegenden Beweise nicht benannt bzw. vollständig offengelegt worden sind, hierzu siehe § 174 Abs. 1 lit. a und b tStPO.

Informationen, sei es von Amts wegen oder auf entsprechenden Antrag der Verteidigung, anordnet. Gängige Praxis ist, dass nachrichtendienstliche Informationen durch einen Bericht (istihbarat raporu/notu) eingeführt werden, der allen Verteidigungsbeteiligten offengelegt wird.

Dadurch, dass die nachrichtendienstlichen Behörden ihre Informationen den Gerichten durch einen Bericht zur Verfügung stellen, sind sie immer noch in der Lage, die eigentlichen Quellen bzw. die Originaldokumente zurückzuhalten. Es ist nicht unüblich, dass die Behörden den Bericht geradezu so aufsetzen, dass dieser im Ergebnis lediglich als Bewertung des Materials oder der Quelle angesehen werden kann, das bzw. die dem Tatgericht nicht offengelegt wird. In anderen Worten beinhalten die Berichte in vielen Fällen auf unspezifiziertem Ursprung basierende Schlussfolgerungen. In der Tat ist die Erstellung eines solchen Berichts für die Nachrichtendienste in der Türkei aus vielen Gründen attraktiv, weil sie dadurch ihre Quellen, Ermittlungsmethoden und sonstige Interessen am besten schützen können.[134] Dadurch können sie nicht nur ihre Informanten geheim halten und deren Wiedereinsetzbarkeit sicherstellen, sondern auch überhaupt für sich behalten, wie sie die in Frage stehenden nachrichtendienstlichen Informationen erlangt haben, etwa ob sie diese durch die Überwachung des Telekommunikationsverkehrs, die technische und personelle Beobachtung oder auch von den ausländischen Nachrichtendienstbehörden erhalten haben. Wie bereits oben erwähnt, deckt sich diese Vorgehensweise auch mit der Auslegung der im MIT-, Polizei- und Gendarmeriegesetz enthaltenen Verwendungsverbote, die sich lediglich auf die „Aufnahmen" beziehen. Durch die Übermittlung der aus diesen „Aufnahmen" entnommenen Informationen in einen Bericht sind die Behörden bestens in der Lage, die gesetzlichen Verwendungsverbote zu schwächen. Insofern ist es fragwürdig, ob diese Verbote einen effektiven Umgehungsschutz gewährleisten können.[135]

Außerdem wirft die Zulassung der nachrichtendienstlichen Berichte die Frage auf, ob das Gericht dadurch dem Aufklärungsgrundsatz und dem Beweisantragsrecht des Beschuldigten Genüge tun kann bzw. tut. In der Praxis lässt sich beobachten, dass die Berichte von den Strafgerichten ohne weitere Aufklärung ihres Ursprungs oder Zustandekommens der gerichtlichen Überzeugungsbildung zugrunde gelegt werden,[136] solange sie nicht die einzigen Beweismittel gegen den Beschuldigten

---

[134] Siehe zum Fall, in dem die polizeilich-nachrichtendienstliche Behörde die Überwachungsdokumente an das Gericht teils geschwärzt übersandte. (Abrufbar unter https://t1p.de/zbmb [Stand: 13.06.2019]).

[135] Weitere praktische Bedenken ergeben sich in diesem Zusammenhang insofern, als die nachrichtendienstliche Überwachung des Telekommunikationsverkehrs und die strafprozessuale von derselben Behörde (BTIK) durchgeführt werden. Auch die Überwachung des MIT kann durch den BTIK implementiert werden, wobei der MIT selbst diese vornehmen kann.

[136] Für die eher schwache Geltung des Beweisantragsrechts des Beschuldigten und des Unmittelbarkeitsprinzips siehe, *Arslan*, Einführung und Übersetzung, S. 33 ff.

darstellen. Somit unterstellen die Gerichte grundsätzlich die Rechtmäßigkeit, Richtigkeit und Vollständigkeit der Berichte.[137] In dieser Hinsicht hat der türkische Kassationsgerichtshof lediglich das bereits angedeutete Verbot entwickelt, wonach die Verurteilung des Beschuldigten nicht ausschließlich auf die nachrichtendienstlichen Informationen gestützt werden darf.[138] Laut dieser Rechtsprechung haben die Berichte der Nachrichtendienste einen schwachen Beweiswert und eine Verurteilung darf beim Nichtvorliegen unterstützenden Beweismaterials nicht ergehen. Damit akzeptiert das Revisionsgericht zweifellos die Berichte der Dienste als zulässiges Beweismittel.[139] Allerdings hat der türkische Kassationsgerichtshof keine etablierte Rechtsprechung, die dem Grundsatz der Amtsaufklärungspflicht sowie dem Beweisantragsrecht der Verteidigung mehr Gewicht beilegen würde,[140] etwa indem er auf der Anhörung des Verfassers eines nachrichtendienstlichen Berichts bestehen würde. Diese auch höchstrichterlich gebilligte Praxis einer extensiven Verwendung der Beweissurrogate läuft Gefahr, das Strafverfahren unter dem Aspekt der gerichtlichen Ermittlungspflicht, bei Beweissurrogaten auf die Herausgabe unmittelbarer Beweismittel durch die Behörden hinzuwirken,[141] im Sinne des Art. 6 Abs. 1 EMRK unfair werden zu lassen. Eine gewisse Hilfestellung könnte die Verfassungsbeschwerde beim türkischen Verfassungsgericht wegen der Verletzung des Rechts auf ein faires Verfahren nach Art. 36 Abs. 1 tVerfG i.V.m. Art. 6 Abs. 1 EMRK gewähren.[142]

Zusammenfassung

Das türkische Recht kennt die funktionale Aufgabenteilung der Sicherheitsbehörden in nachrichtendienstliche Tätigkeiten (istihbarat), polizeiliche Gefahrenabwehr (önleme) und Strafverfolgung (ceza takibi). Vier Nachrichtendienste tragen zur

---

[137] Hinzukommt, dass das türkische Strafprozessrecht keine Unterscheidung zwischen dem Streng- und Freibeweisverfahren kennt, hierzu siehe *Arslan*, Einführung und Übersetzung, S. 36 f.

[138] Zur entsprechenden Rechtsprechung siehe 10. YCD Entsch. v. 27.03.2008 E. 2007/25667 K. 2008/4879; 10. YCD Entsch. v. 25.05.2011 E. 2011/5104 K. 2011/4583; in diese Richtung auch YCGK Urt. v. 17.11.2009 E. 2009/7-160 K. 2009/364.

[139] Obwohl immer wieder einige Richter am türkischen Kassationsgerichtshof in ihren Minderheitsvoten den nachrichtendienstlichen Berichten mit der Begründung die Zulässigkeit gänzlich abzusprechen versuchen, dass diese Berichte „einseitig, nicht sachdienlich, nicht geprüft und nur Informationen aus zweiter Hand" seien, ist die Mehrheitsmeinung eher gegenteiliger Auffassung, siehe hierzu die Entscheidung von Yargıtay 10. CD, 28.06.2013, 2012/490, 2013/6666.

[140] Nach dem EGMR müssen auch in solchen Fällen die Verteidigungsrechte, insbesondere die Gelegenheit zum Widerspruch gegen die Richtigkeit der in Frage stehenden Beweise und deren Verwendung, gewährleistet werden; siehe Satık v. Türkei, No: 60999/00, 08 Oktober 2018, § 55. Mehr dazu siehe *Birtek*, CHD 2011, 123 ff.

[141] EGMR Georgios Papageorgiou ./. Griechenland Urt. v. 09.05.2003 §§ 35 ff.

[142] Hierzu siehe *Arslan*, Staatsgeheimnisse, S. 52 ff.

Gewährleistung der nationalen Sicherheit bei (der Nationale Nachrichtendienst: MIT und die Nachrichtendienstdirektion des Generalstabs: GIDB) und der Förderung der Gefahrenabwehr und Strafverfolgung (die Nachrichtendienstdirektion der Polizei: EIDB und das Nachrichtendienstpräsidium der Gendarmerie: JIB). Die Kommission zur Ermittlung von Finanzkriminalität (MASAK) versteht sich in letzter Zeit ebenfalls als ein echter Finanznachrichtendienst.

Mit der Gesetzesänderung im Jahr 2014 erweiterten sich die Befugnisse des MIT um mehrere wesentliche Aspekte. So ist es ihm nun gestattet, Ausland-Ausland- sowie Ausländer-Aufklärung zu betreiben. Hinzu kommt, dass seit der Gesetzesänderung auch die Erfüllung präsidialer Anweisungen im Bereich der äußeren und nationalen Sicherheit und die Terrorismusbekämpfung zu den Aufgaben des MIT gehört. In diesem Zusammenhang steht es dem MIT zu, Gespräche mit illegalen und terroristischen Vereinigungen zu führen sowie von einschlägigen Koordinationsmaßnahmen Gebrauch zu machen. Um weitere ausdrücklich exekutive Befugnisnormen, die den MIT zur Anwendung unmittelbaren Zwangs ermächtigen würden, wurde das MIT-Gesetz nicht ergänzt.

Was die Aufgaben der EIDB und des JIB angeht, so lässt sich konstatieren, dass ein gesetzliches Unterscheidungskriterium zwischen der nachrichtendienstlichen Informationssammlung im Hinblick auf unspezifische mögliche Gefahren und der Gefahrenabwehr im Einzelfall fehlt. Beides wird ohne eine weitere Unterscheidung als Gefahrenprävention (tehlikenin önleme) aufgefasst. Zu der unklar gezogenen funktionalen Aufgabenbestimmung zwischen der nachrichtendienstlichen Informationssammlung und der Gefahrenabwehr im Einzelfall kommt hinzu, dass auch die Strafverfolgung von den Behörden betrieben wird, bei denen auch die EIDB und das JIB angesiedelt sind. Dies hat u.a. zur Folge, dass die drei Aufgabenarten jeweils von Beamten erledigt werden, die dieselben Rechte und Pflichten haben. Insofern besteht auf der Ebene der Polizei und Gendarmerie ein sehr enges organisatorisches und personelles Zusammentreffen der nachrichtendienstlichen Informationssammlung und der Strafverfolgung.

Bei der fehlenden Trennung hinsichtlich der Inlandsnachrichtendienste in der Türkei besteht nicht nur die Gefahr, dass die primär nachrichtendienstliche Informationssammlung vernachlässigt wird, weil der Fokus auf die Operationalisierung der gesammelten Informationen, sei es durch die Gefahrenabwehr im Einzelfall oder auch die Strafverfolgung, gelegt wird, sondern auch die des Machtmissbrauchs und der Umgehung strafprozessualer Garantien.[143]

Was die Übermittlung nachrichtendienstlicher Informationen an die Strafverfolgung angeht, so lässt sich für den MIT feststellen, dass es grundsätzlich in seinem Ermessen liegt, eine entsprechende Übermittlung von sich aus oder auf Anfrage der

---

[143] Vgl. *Özbek,* DEÜHFD 2002, S. 85; siehe auch AYM, No: 2013/533, 9.1.2014, para. 60. Amtsblatt: 25 Februar 2014–28924.

Strafverfolgungsbehörden vorzunehmen. Sein Ermessen erstreckt sich grundsätzlich auch auf die Umstände, bei welchem Verdachtsgrad und hinsichtlich welcher Straftaten die Informationen zu übermitteln sind. § 6 Abs. 6 des MIT-Gesetzes schränkt jedoch das Ermessen des MIT dahingehend ein, dass etwa die Verwendung der durch die strategischen, individuellen, Ausland-Ausland-, Ausländer-, und anonymen TKÜs erlangten „Aufnahmen" außer zu den in diesem Gesetz genannten Zwecken verboten ist. Bei näherem Hinsehen stellt sich allerdings heraus, dass sich das Verwendungsverbot lediglich auf die Aufnahmen als solche erstrecken und die hieraus gewonnenen nachrichtendienstlichen Informationen bzw. deren Auswertungen nicht darunterfallen. Diese können etwa durch einen Bericht an die Staatsanwaltschaft oder auch an die Gerichte übermittelt werden. Das entsprechende Ermessen des MIT zeigt sich auch dadurch, dass der Präsident des MIT im Hinblick auf die Angehörigen seines Dienstes oder andere Personen, die für den MIT Aufträge erfüllt haben (etwa Informanten), die Aussagegenehmigung verweigern kann, wenn er dies zum Schutz von Dienstgeheimnissen oder anderweitigen staatlichen Interessen für erforderlich hält. Desgleichen sieht das MIT-Gesetz vor, dass die Justizinstanzen einschließlich der Strafgerichte vom MIT die Übermittlung nachrichtendienstlicher Informationen oder die Herausgabe von anderweitigem Material nicht anfordern dürfen. Dieses Anforderungsverbot schließt allerdings nicht aus, dass die Justizinstanzen formlose Anfragen stellen, über die der MIT nach seinem Ermessen entscheiden wird.

Auch hinsichtlich der Informationsübermittlung durch die EIDB und das JIB an die Strafverfolgungsbehörden besteht ein weitgehendes Ermessen dieser beiden Behörden. Bei näherer Betrachtung stellt sich heraus, dass diese beiden Inlandsnachrichtendienste konzeptionell derart aufgestellt sind, dass sie mit den Strafverfolgungsbehörden nicht zuletzt durch die Übermittlung nachrichtendienstlicher Informationen eng zusammenarbeiten. Betrachtet man auch die organisatorische und personelle Nähe zwischen diesen Diensten und den Strafverfolgungsbehörden, so kann man auch von einer gewissen Einheit sprechen, die sich unter anderem in einigen Bereichen der Kriminalität durch einen regen Informationsaustausch auszeichnet. Dieser konzeptionellen Aufstellung entspricht auch der Zustand, dass das türkische Nachrichtendienstrecht kein Anforderungsverbot für die Justizinstanzen enthält, wenn es um die Auskunftsanfragen an die EIDB und das JIB geht. Dagegen gilt auch ein Verbot für die Verwendung der Aufnahmen im Strafprozess, die die beiden Dienste etwa durch technische Mittel – grundsätzlich nachrichtendienstliche TKÜ – erlangt haben. Allerdings ist auch hier die Reichweite des Verwendungsverbots dahingehend begrenzt, dass nur die Aufnahmen als solche darunterfallen, die daraus gewonnenen Informationen und Auswertungen dagegen nicht.

Im Strafverfahren ist die Staatsanwaltschaft nach § 161 Abs. 1 befugt, abgesehen vom MIT, nachrichtendienstliche Informationen bei der EIDB und dem JID einzufordern. Das Anforderungsverbot nach dem Zusatzparagraph 1 des MIT-Gesetzes besteht nur bei Straftaten gegen Staatsgeheimnisse und Spionage (§§ 326 ff. tStGB) nicht. Schwierigkeiten bei der Verteidigung entstehen dem Beschuldigten, wenn die

Staatsanwaltschaft die Verwendung nachrichtendienstlicher Informationen bei der Anordnung von Ermittlungsmaßnahmen oder auch bei der Erhärtung eines für die Anklage hinreichenden Verdachts nicht offenlegt. Im Hauptverfahren ergeben sich Schwierigkeiten für die Verteidigung in der Regel dann, wenn die nachrichtendienstlichen Berichte (istihbarat raporu) herangezogen werden, deren Rechtsmäßigkeit und Verlässlichkeit die Verteidigung jedoch nicht anzufechten vermag.

Literaturverzeichnis

Arslan, Çetin, Intelligence in Criminal Procedure Law. ABD 2013/2, 5–64.

Arslan, Mehmet, Die türkische Strafprozessordnung. Deutsche Übersetzung und Einführung. Berlin 2017.

Arslan, Mehmet, Intelligence and Crime Control in the Security Law of Germany. In: Dyson, Matthew/Vogel, Benjamin (Hrsg.), The Limits of Criminal Law. Cambridge 2018, S. 507–536.

Arslan, Mehmet, Staatsgeheimnisse im türkischen Strafverfahren. Freiburg im Breisgau 2017.

Arslan, Mehmet, Weltweite Telekommunikationsüberwachung durch Geheimdienste im Spiegelbild der kantischen Idee zum Ewigen Frieden. KritV, 2018/4, 287–311.

Aybay, Rona, Milli Güvenlik Kavramı ve Milli Güvenlik Kurulu. AÜSBFD, 33 (1) 1978, 59–82.

Birtek, Fatih, İstihbarat Amacıyla İletişim Özgürlüğüne Müdahale Edilmesi ve Müdahaleden Elde Edilen Materyallerin Delil Olarak Kabul Edilebilirliği, CHD, 6 (16), 2011, 100–148.

Fidan, Hakan, Intelligence and Foreign Policy: A Comparison of British, American and Turkish Intelligence Systems, Masterarbeit, Universität Bilkent. Ankara 1999.

Kuloğlu, Gökhan, Organize Suç İstihbaratı Operasyon Yönetimi ve Bir Model Önerisi. PBD, 14 (4) 2012, 1–30.

Külçür, Erdem İzzet, Uluslararası Suçlar, Sınıraşan Suçlar ve Yabancılık Unsuru Kavramlarına Dar ve Geniş Anlamda Bir Bakış. SCD, 1 (2) 2016, 7–46.

Özbek, Veli Özer, et al., Ceza Muhakemesi Hukuku. Ankara 2018.

Özbek, Veli Özer, Organize Suçlulukla Mücadelede Ön Alan Soruşturmaları, DEÜHFD, 4 (2) 2002, 57–88.

Pınarbaşı, Mesut, Özel Hayatın Korunması Kapsamında İstihbarat Faaliyetlerinin Hukuksal Sınırları, Yüksek Lisans Tezi, Kara Harp Okulu Savunma Bilimleri Enstitüsü, 2014.

Seyhan, Kazım/Eryılmaz, M. Bedri, Gelişmiş Ülkeler ve Türkiye Uygulamasında Suç Önleme Stratejileri. LD, Bahar 2004, 5–34.

Şahin, Cumhur, Telekomünikasyon Yoluyla İletişimin Denetlenmesi – Yargıtay Kararları Çerçevesinde Bir Değerlendirme-. GÜHFD, C. XI, Sa. 1–2 2007, 1095–1112.

Tellenbach, Silvia, Das türkische Strafgesetzbuch, Berlin 2008.

Turhan, Faruk/Aksu, Muharrem, İnsan Haklarının Korunması Açısından Önleyici Amaçlı İletişimin Denetlenmesi Tedbiri. Uluslararası Davraz Kongresi Bildiri Kitabı, 2009.

Yenisey, Feridun, Kolluk Hukuku [Polizeirecht], Istanbul 2015.

Gesetzestexte

Auszüge aus dem Gesetz über die nachrichtendienstlichen Dienste des Staates und den Nationalen Nachrichtendienst (MIT-Gesetz)

Aufgaben des Nationalen Nachrichtendienstes

§ 4 – Der Nationale Nachrichtendienst hat folgende Aufgaben:

a) im Hinblick auf die vorhandenen oder möglichen Aktivitäten, die sich aus dem Inland oder Ausland gegen die Integrität der Türkischen Republik als Land und Nation, deren Bestand, Unabhängigkeit, Sicherheit, Verfassungsordnung und alle Bestandteile der nationalen Schlagkraft richten, landesweit das nationale Nachrichtenwesen zu etablieren und die entsprechenden Informationen dem Staatspräsidenten, dem Generalstabchef, dem Sekretariat des Nationalen Sicherheitsrats sowie anderen einschlägigen Behörden zukommen zu lassen,

b) bei der Vorbereitung der die nationale Sicherheitspolitik des Staates betreffenden Vorhaben und deren Umsetzen die Ersuchen und Anforderungen des Staatspräsidenten, des Generalstabchefs, des Sekretariats des Nationalen Sicherheitsrats zu erfüllen,

c) zur Steuerung der nachrichtendienstlichen Tätigkeiten der öffentlichen Körperschaften und Anstalten dem Staatspräsidenten und dem Nationalen Sicherheitsrat Vorschläge zu unterbreiten,

d) bei Maßnahmen der öffentlichen Körperschaften und Anstalten, die die Sammlung von Informationen oder die Spionageabwehr betreffen, in technischen Angelegenheiten Beratung und für die Herstellung der Koordination Hilfe zu leisten,

e) Nachrichten und Informationen, die der Generalstabschef für die Streitkräfte benötigt, entsprechend einer zu erzielenden Vereinbarung dem Generalstabchef zukommen zu lassen,

f) Andere Aufgaben, die der Nationale Sicherheitsrat bestimmt, zu erledigen,

g) Spionageabwehr,

h) (eingefügt am 17.4.2014 durch § 1 des Gesetzes Nr. 6532) Aufträge des Staatspräsidenten, die die äußere Sicherheit, die Bekämpfung des Terrorismus und die nationale Sicherheit betreffen, zu erfüllen,

i) (eingefügt am 17.4.2014 durch § 1 des Gesetzes Nr. 6532) im Hinblick auf die nachrichtendienstliche Tätigkeiten bezüglich des Auslands, der nationalem Verteidigung, der Terrorbekämpfung, der internationalen Straftaten sowie der Cyberstraftaten Informationen, Dokumente, Nachrichten, Angaben mithilfe technischer oder personenbasierter nachrichtendienstlicher Vorgehensweisen, Mitteln und Systemen zu sammeln, zu speichern, zu analysieren und die generierten Erkenntnisse den betreffenden Behörden zukommen zu lassen

j) (eingefügt am 17.4.2014 durch § 1 des Gesetzes Nr. 6532) moderne nachrichtendienstliche Vorgehensweisen und Methoden zu erforschen, technische Entwicklungen zu

verfolgen und die angewandten zu beschaffen, damit die Kapazität der Informationssammlung, deren Qualität sowie Effektivität erhöht werden.

(Geänderter Satz vom 17.4.2014 durch § 1 des Gesetzes Nr. 6532) Dem Nationalen Nachrichtendienst darf außer den genannten keine andere Aufgabe übertragen werden. Die Aufgaben, Befugnisse und Verantwortlichkeit der einzelnen Einheiten des Nationalen Nachrichtendienstes werden durch eine Rechtsverordnung bestimmt, die der Zustimmung des Staatspräsidenten bedarf.

Befugnisse

§ 6 – (Geänderter erster Absatz vom 17.4.2014 durch § 3 des Gesetzes Nr. 6532) Der Nationale Nachrichtendienst macht bei der Erfüllung der in diesem Gesetz genannten Aufgaben von folgenden Befugnissen Gebrauch:

a) zu einheimischen und ausländischen Körperschaften und Anstalten aller Art, allen Vereinigungen oder Zusammenschüsse und Personen unmittelbar in Kontakt zu treten und von einschlägigen Koordinationsmaßnahmen Gebrauch zu machen,

b) von öffentlichen Körperschaften und Anstalten, Berufsverbänden mit der Eigenschaft einer öffentlichen Körperschaft, Körperschaften und Anstalten nach dem Bankengesetz von 19.10.2005 mit der Nr. 5411 und anderen juristischen Personen sowie Verbänden, die keine juristische Personen sind, Informationen, Dokumente, Daten und Aufnahmen zu erhalten, von deren Archiven, elektronischen Informationsverwaltungssystemen, Kommunikationsinfrastrukturen zu profitieren und zu diesen in Kontakt zu treten. Die in diesem Zusammenhang Ersuchten dürfen die Erfüllung des Ersuchens mit dem Hinweis auf ihre eigene Gesetzgebung nicht verweigern,

c) im Ermittlungs- und Hauptverfahren, die in vierten, fünften, sechsten und siebten Abschnitten des vierten Teiles des zweiten Buches des türkischen Strafgesetzbuches (außer §§ 318, 319, 324, 325, 332) genannten Straftaten betreffen, Zugang zu Vernehmungsschriften und Dokumenten sowie Belegen aller Art zu erhalten und Abschriften von diesen zu nehmen,

d) geheime Arbeitsmethoden, Prinzipien und Techniken bei der Erfüllung ihrer Aufgaben heranzuziehen,

e) die Identität der für nachrichtendienstlichen Zwecken eingesetzten Personen zu ändern, für deren Geheimhaltung alle Maßnahmen zu ergreifen und juristische Personen zu gründen. Erforderliche Dokumente, Aufnahmen und Urkunden sowie Fahrzeuge und Werkzeuge dürfen zur Verfügung gestellt, geändert und benutzt werden, wenn dies für die Bildung einer Legende sowie die Gründung einer juristischen Person und deren Fortsetzung erforderlich sind,

f) im Zusammenhang mit der Ein- und Ausreise von Ausländern sowie Bewilligung eines Visums, einer Aufenthalts- oder Arbeitserlaubnis und Ausweisungen betreffende Körperschaften und Anstalten zu ersuchen,

g) aus den Telekommunikationsleitungen Angaben, die das Ausland, die nationale Verteidigung, Terrorismus und internationale Straftaten betreffen, zu sammeln,

h) Unternehmungen zu tätigen, die auf die Unterbindung der Aktivitäten fremder Elemente hinzielen, die Kommunikationssicherheit des Landes und der Bürger gefährden, und betreffende Körperschaften und Anstalten zu ersuchen,

i) von Prüfmethoden- und Verfahren einschließlich des Einsatzes eines Lügendetektors Gebrauch zu machen, um die Vertrauenswürdigkeit und Geeignetheit der Personen, bei beim MIT beschäftigt sind oder für eine Beschäftigung in Frage kommen, festzustellen,

j) MIT-Angehörige dürfen bei der Erfüllung ihrer Aufgaben verhaftete und verurteilte Personen, die sich in Justizvollzugsanstalten befinden, nach einer vorausgehenden Benachrichtigung besuchen, andere Personen zum Besuch bringen und alle Zusammenschlüsse

einschließlich der Terrororganisationen, die die nationale Sicherheit bedrohen, zu kontaktieren.

(Eingefügt am 03.07.2005 durch § 3 des Gesetzes Nr. 5397) Im Rahmen der Erfüllung der in § 4 dieses Gesetzes aufgelisteten Aufgaben und zum Zwecke der Gewährleistung der Staatssicherheit, der Aufdeckung von Spionagetätigkeiten, der Ermittlung von Offenlegungen von Staatsgeheimnissen und der Verhinderung der terroristischen Aktivitäten kann die Telekommunikation durch einen richterlichen Beschluss und bei Gefahr im Verzug durch eine schriftliche Anweisung des Präsidenten der Dienstes oder dessen Stellvertreter festgestellt, abgehört, gespeichert und deren Verkehrsdaten ausgewertet werden, wenn eine ernsthafte Gefahr für die im Art. 2 der Verfassung bestimmten Grundeigenschaften und den demokratischen Rechtstaat vorliegt. Eine schriftliche Anweisung, die bei Gefahr im Verzug erteilt wurde, ist innerhalb von 24 Stunden dem örtlich und sachlich zuständigen Richter vorzulegen. Der Richter fällt seine Entscheidungen spätestens innerhalb von 24 Stunden. Ist diese Frist verstrichen oder verwirft der Richter den Antrag, so wird die Maßnahme sofort aufgehoben. In diesem Fall müssen Aufnahmen von den Abhörinhalten spätestens innerhalb von zehn Tagen vernichtet werden. Dies wird mit einem Protokoll festgehalten und das Protokoll wird aufbewahrt, um bei Kontrollen vorgelegt werden zu können. Diese Schritte werden von der Stelle, die vom MIT gegründet wurde, oder von der Stelle, die entsprechend dem Zusatzparagraphs 7 Abs. 10 des Gesetzes über Aufgaben und Befugnisse der Polizei vom 04.07.1934 mit der Nr. 2559 gegründet wurde, in die Wege geleitet. (Geänderter letzter Satz vom 04.05.2009 durch § 12 des Gesetzes Nr. 5651) Telekommunikationsüberwachungen, die nach § 135 Abs. 6 lit. a Nr. 14 der Strafprozessordnung v. 04.12.2004 mit der Nr. 5271 vorzunehmen sind, werden ebenfalls von diesen Stellen durchgeführt.

(Eingefügter Absatz am 03.07.2005 durch § 3 des Gesetzes Nr. 5359; geänderter dritter Absatz vom 17.04.2014 durch das Gesetz Nr. 6532) Der örtlich und sachlich zuständige Richter ist ein Mitglied des Gerichts für schwere Straftaten in Ankara.

(Eingefügter Absatz am 03.07.2005 durch § 3 des Gesetzes Nr. 5397) Im Beschluss oder der schriftlichen Anweisung sind die Personalien der von der Maßnahme betroffenen Person, die Art ihres Telekommunikationsmittels, die von ihr benutzten Telefonnummern oder andere bestimmbare Codes, die die Feststellung ihrer Telekommunikation ermöglichen würden, die Art, die Reichweite, die Dauer der Maßnahme sowie die Gründe für das Ergreifen dieser Maßnahme anzugeben. Die Entscheidungen dürfen für höchstens drei Monate getroffen werden. Diese Frist darf im Wege desselben Verfahrens jeweils um weitere drei Monate und höchstens dreimal verlängert werden. Allerdings darf der Richter die Frist jeweils um weitere drei Monate wiederholt verlängern, wenn dies aufgrund der Gefahren, die sich aus den fortdauernden Spionage- oder Terroraktivitäten ergeben, für erforderlich gehalten wird.

(Eingefügter Absatz am 03.07.2005 durch § 3 des Gesetzes Nr. 5397) Wird die ergriffene Maßnahme beendet, so werden die Inhalte des Abhörens spätestens innerhalb von zehn Tagen vernichtet. Dies wird mit einem Protokoll festgehalten und das Protokoll wird aufbewahrt, um bei Kontrollen vorgelegt werden zu können.

(Eingefügter Absatz am 03.07.2005 durch § 3 des Gesetzes Nr. 5397) Aufnahmen, die im Rahmen der nach diesem Paragraphen durchgeführten Maßnahmen erlangt werden, dürfen außer zu den in diesem Paragraphen genannten Zwecken nicht verwendet werden. Für die Aufbewahrung und den Schutz der erlangten Informationen gilt das Geheimhaltungsprinzip. (Gestrichener letzter Satz am 17.04.2014 durch § 3 des Gesetzes Nr. 6532)

(Eingefügter Absatz am 03.07.2005 durch § 3 des Gesetzes Nr. 5397) Der richterliche Beschluss und die schriftliche Anweisung werden von Bediensteten des MIT umgesetzt. Das Datum und die Uhrzeit des Beginns sowie das Ende der Maßnahme sowie die Personalien der ausführenden Person sind in einem Protokoll festzuhalten.

(Eingefügter Absatz am 03.07.2005 durch § 3 des Gesetzes Nr. 5397) Die nach diesem Paragraphen durchgeführten Maßnahmen werden durch die behördlichen Vorgesetzen nach ihren Rangverhältnissen und durch die Staatliche Aufsichtsbehörde kontrolliert.

(Eingefügter Absatz am 03.07.2005 durch § 3 des Gesetzes Nr. 5397) Abhörmaßnahmen, die entgegen der in diesem Paragraphen bestimmten Verfahren und Grundsätze durchgeführt werden, sind rechtsunwirksam, und auf die Personen, die in dieser Weise Abhörmaßnahmen vorgenommen haben, ist das türkische Strafgesetzbuch vom 26.09.2004 Nr. 5237 anzuwenden.

(Eingefügter Absatz am 03.07.2005 durch § 3 des Gesetzes Nr. 5397; geändert am 02.07.2018 durch § 152 des Ausnahmezustandsdekrets Nr. 703) Verfahren und Grundsätze, die die Anwendung dieses Paragraphs betreffen, sind durch eine vom Staatspräsidenten zu erlassende Rechtsverordnung zu regeln.

(Eingefügter Absatz am 17.4.2014 durch § 3 des Gesetzes Nr. 6532) Unabhängig von den oben aufgeführten Bestimmungen sowie anderen Gesetzen, die auf die präemptive Informationssammlung und Analyse abzielen, dürfen die im Ausland oder von den Ausländern getätigte Kommunikation sowie die aus den Münzfernsprechern getätigte Kommunikation und die Kommunikation jener Personen, die Angehörige des MIT sind, beim MIT Aufgaben übernommen hatten oder sich für eine Beschäftigung beim MIT bewerben, durch die Genehmigung des Präsidenten des Dienstes oder dessen Stellvertreter festgestellt, abgehört, gespeichert und deren Verkehrsdaten ausgewertet werden.

(Eingefügter Absatz am 17.4.2014 durch § 3 des Gesetzes Nr. 6532) Die Verfahren und Prinzipien, die die Erfüllung der in diesem Gesetz genannten Aufgaben sowie die Ausübung der Befugnisse betreffen, sind durch eine Rechtsverordnung zu regeln.

Es wird durch eine Rechtsverordnung geregelt, welchen MIT-Angehörigen bei der Erfüllung der in diesem Gesetz genannten Aufgaben jene Rechte und Befugnisse zustehen, die der allgemeinen Polizei eingeräumt sind.

Zeugenschaft

§ 29 (Geändert am 15.08.2017 durch § 76 des Ausnahmezustandsdekrets Nr. 694; angenommen in gleicher Fassung am 01.02.2018 durch § 72 des Gesetzes Nr. 7078)

MIT-Angehörige oder jene Personen, die Aufträge für den MIT erfüllt haben, benötigen eine Genehmigung des Präsidenten des Dienstes, wenn sie als Zeuge aussagen sollen und staatliche Interessen oder die Geheimhaltungsbedürfnisse ihrer Aufgaben dies erfordern; der Präsident des Dienstes benötigt eine Genehmigung des Staatspräsidenten.

Zusatzparagraph 1 (Eingefügt am 17.04.2014 durch § 11 des Gesetzes Nr. 6532)

Informationen, Dokumente, Angaben, Aufnahmen sowie durchgeführte Analysen, die nachrichtendienstlich und im Besitz des Nationalen Nachrichtendienst sind, dürfen, abgesehen von Straftaten, die im siebten Abschnitt des vierten Teils des zweiten Buchs des türkischen Strafgesetzbuchs definiert sind, von justiziellen Stellen nicht angefordert werden.

Auszüge aus dem Gesetz über Aufgaben und Befugnisse der Polizei (PVSK)

§ 2 (Geändert am 16.07.1965 durch § 2 des Gesetzes Nr. 694)

Aufgaben der Polizei, die die allgemeine Sicherheit betreffen, sind zweierlei:

A) Handlungen, die den Gesetzen, den Präsidialdekreten, Rechtsverordnungen, Regierungsverfügungen und der öffentlichen Ordnung zuwiderlaufen, bereits vor deren Begehung nach Maßgabe dieses Gesetzes vorzubeugen,

B) Bei einer begangenen Straftat Aufgaben zu übernehmen, die in der Strafprozessordnung sowie in anderen Gesetzen genannt sind,

…

Zusatzparagraph 7 (Eingefügt am 16.06.1985 durch § 7 des Gesetzes Nr. 3233)

Die Polizei betreibt landesweit und im virtuellen Raum nachrichtendienstliche Tätigkeiten, sammelt zu diesem Zweck Informationen, wertet diese aus, lässt sie den zuständigen Instanzen oder dem Verwendungsbereich zukommen, um präventive und schützende Maßnahmen hinsichtlich der Integrität des Staates als Land und Nation, der Verfassungsordnung und der allgemeinen Sicherheit zu ergreifen und die Sicherheit und den Frieden zu gewährleisten. Sie arbeitet mit anderen Nachrichtendiensten des Staates zusammen.

(Eingefügter Absatz am 03.07.2005 durch § 1 des Gesetzes Nr. 5397) Zur Erfüllung der im ersten Absatz genannten Aufgaben und zur Vorbeugung der in § 250 Abs. 1 lit. a, b und c der Strafprozessordnung v. 04.12.2004 Nr. 5271 genannten Straftaten (Spionagestraftaten ausgenommen)[144] sowie der Cyberstraftaten dürfen auf einen richterlichen Beschluss hin oder bei Gefahr im Verzug auf die schriftliche Anweisung des Polizeipräsidenten, des Präsidenten der Nachrichtendienstdirektion der Polizei oder, auf die Cyberstraftaten beschränkt, des Präsidenten der betreffenden Direktion hin der durch die Telekommunikation getätigte Kommunikationsverkehr und die Daten, der durch den zwischen den Internetverbindungsadressen und den Internetquellen getätigte Datenverkehr übermittelt werden, festgestellt, abgehört, gespeichert und dessen Signaldaten ausgewertet werden. Eine schriftliche Anweisung, die bei Gefahr im Verzug erteilt wurde, ist innerhalb von 24 Stunden dem örtlich und sachlich zuständigen Richter vorzulegen. Der Richter fällt seine Entscheidungen spätestens innerhalb von 48 Stunden. Ist diese Frist verstrichen oder verwirft der Richter den Antrag, so wird die Maßnahme sofort aufgehoben. In diesem Fall sind Aufnahmen von Abhörinhalten spätestens innerhalb von zehn Tagen zu vernichten. Dies wird mit einem Protokoll festgehalten und das Protokoll wird aufbewahrt, um bei Kontrollen vorgelegt werden zu können.

(Eingefügter Absatz am 03.07.2005 durch § 1 des Gesetzes Nr. 5359; geänderter Absatz vom 07.03.2015 durch § 5 des Gesetzes Nr. 6638) Der örtlich und sachlich zuständige Richter ist ein Mitglied des Gerichtes für schwere Straftaten in Ankara.

(Eingefügter Absatz am 03.07.2005 durch § 1 des Gesetzes Nr. 5397) Im Beschluss oder der schriftlichen Anweisung sind die Personalien der von der Maßnahme betroffenen Person, die Art ihres Telekommunikationsmittels, die von ihr benutzten Telefonnummern, die einschlägige Internetverbindungsadresse oder andere bestimmbare Codes, die die Feststellung ihrer Verbindung ermöglichen würden, die Art, die Reichweite, die Dauer der Maßnahme sowie die Gründe für das Ergreifen dieser Maßnahme anzugeben. Die Entscheidungen dürfen für höchstens drei Monate getroffen werden. Diese Frist darf im Wege desselben Verfahrens jeweils für weitere drei Monate und höchstens dreimal verlängert werden. Allerdings darf der Richter die Frist jeweils um weitere drei Monate wiederholt verlängern, wenn dies aufgrund der Gefahren, die sich aus den fortdauernden Terroraktivitäten ergeben, für erforderlich gehalten wird.

(Eingefügter Absatz am 03.07.2005 durch § 1 des Gesetzes Nr. 5397) Wird die ergriffene Maßnahme beendet, so werden die Inhalte des Abhörens spätestens innerhalb von zehn Tagen vernichtet. Dies wird mit einem Protokoll festgehalten und das Protokoll wird aufbewahrt, um bei Kontrollen vorgelegt werden zu können.

(Eingefügter Absatz am 03.07.2005 durch § 1 des Gesetzes Nr. 5397) Im Rahmen der nachrichtendienstlichen Tätigkeiten darf zur Vorbeugung der in diesem Paragraphen genannten

---

[144] Diese Straftaten sind nach § 1 Abs. 6 des Änderungsgesetzes vom 21.02.2016 mit Nr. 6526 folgende aus dem türkischen Strafgesetzbuch; a) im Rahmen einer kriminellen Organisation begangene Herstellung und Handel mit Betäubungsmitteln und Geldwäsche, b) im Rahmen einer kriminellen Organisation zum Zwecke der Erlangung illegalen Profits mit Nötigung und Bedrohung begangegene Straftaten, c) im zweiten Buch des vierten Teils der vierten, fünften, sechsten und siebten Abschnitten definierte Straftaten (Paragraphen 305, 318, 319, 323, 324, 325 und 332 ausgenommen).

Straftaten und durch einen richterlichen Beschluss eine Beobachtung durch technische Mitteln vorgenommen werden. Außerdem dürfen bei den öffentlichen Körperschaften und Anstalten sowie Einrichtungen, die öffentliche Dienste anbieten, für den dienstlichen Gebrauch unter Angabe von Gründen schriftlich benötigte Informationen und Dokumente angefragt werden. Geben diese Körperschaften und Anstalten-Einrichtungen aus gesetzlichen Gründen oder Gründen der Geschäftsgeheimnisse die betreffenden Informationen und Dokumente nicht heraus, so dürfen diese nur durch einen richterlichen Beschluss herangezogen werden.

(Eingefügter Absatz am 03.07.2005 durch § 1 des Gesetzes Nr. 5397) Aufnahmen, die im Rahmen der nach diesem Paragraphen durchgeführten Maßnahmen erlangt werden, dürfen außer zu den in diesem Paragraphen genannten Zwecken nicht verwendet werden. Für die Aufbewahrung und den Schutz der erlangten Informationen gilt das Geheimhaltungsprinzip. Gegen die Personen, die gegen Bestimmungen dieses Absatzes verstoßen haben, dürfen Strafermittlungen unmittelbar von Staatsanwälten durchgeführt werden, auch wenn die Verstöße während des Dienstes oder aufgrund des Dienstes begangen wurden.

(Eingefügter Absatz am 03.07.2005 durch § 1 des Gesetzes Nr. 5397) Der richterliche Beschluss und die schriftliche Anweisung werden von Bediensteten der Nachrichtendirektion der Polizei oder, auf die Cyberstraftaten beschränkt, von Bediensteten der zuständigen Direktion umgesetzt. Das Datum und die Uhrzeit des Beginns sowie des Endes der Maßnahme sowie die Personalien der ausführenden Person sind in einem Protokoll festzuhalten.

(Eingefügter Absatz am 03.07.2005 durch § 3 des Gesetzes Nr. 5397) Die nach diesem Paragraph durchgeführten Maßnahmen werden durch die behördlichen Vorgesetzen nach ihren Rangverhältnissen, die Vorgesetzen der jeweiligen Verwaltungseinheit, der Polizeigeneraldirektion und durch das Inspektionspersonal des betreffenden Ministeriums jährlich mindestens einmal kontrolliert. Diese Maßnahmen dürfen auch vom Aufsichtsausschuss des Ministeramtes kontrolliert werden. Die Ergebnisse der in diesem Rahmen getätigten Kontrollen werden durch einen Bericht dem Sicherheits- und Nachrichtendienstausschuss der Türkischen Nationalversammlung vorgelegt.

(Eingefügter Absatz am 03.07.2005 durch § 1 des Gesetzes Nr. 5397; geändert am 15.08.2016 durch § 24 des Ausnahmezustandsdekrets Nr. 671; angenommen in derselben Fassung am 09.11.2016 durch § 21 des Gesetzes Nr. 6757) Die nach diesem Paragraphen ergriffenen Maßnahmen bezüglich der Telekommunikation sowie die nach § 135 des Gesetzes Nr. 5271 zu tätigenden Abhörmaßnahmen sind unter dem Dach der Behörde für Informationstechnologien und Kommunikation von einer Stelle vorzunehmen.

(Eingefügter Absatz am 03.07.2005 durch § 1 des Gesetzes Nr. 5397) Abhörmaßnahmen, die entgegen die in diesem Paragraphen bestimmten Verfahren und Grundsätze durchgeführt werden, sind rechtsunwirksam, und auf die Personen, die in der Weise Abhörungen getätigt haben, ist das türkische Strafgesetzbuch vom 26.09.2004 Nr. 5237 anzuwenden.

(Eingefügter Absatz am 03.07.2005 durch § 1 des Gesetzes Nr. 5397) Verfahren und Grundsätze, die die Anwendung dieses Paragraphs betreffen, sind durch eine vom Staatspräsidenten zu erlassende Rechtsverordnung zu regeln.

Auszüge aus dem JTGYK

Zusatzparagraph 5 (Eingefügter Absatz am 03.07.2005 durch § 2 des Gesetzes Nr. 5397)

Im Rahmen der Erfüllung der in § 7 lit. a dieses Gesetzes genannten Aufgaben, zum Ergreifen der vorbeugenden und schützenden Maßnahmen und, begrenzt auf seinen Zuständigkeitsbereich, zur Vorbeugung der in § 250 Abs. 1 lit. a, b und c der Strafprozessordnung v.

04.12.2004 mit der Nr. 5271 genannten Straftaten (Spionagestraftaten ausgenommen)[145] darf auf einen richterlichen Beschluss hin oder bei Gefahr im Verzug auf die schriftliche Anweisung des Stabschefs der Gendarmerie oder des Präsidenten der Nachrichtendienstdirektion hin der durch die Telekommunikation getätigte Kommunikationsverkehr festgestellt, abgehört, gespeichert und dessen Signaldaten ausgewertet werden. Eine schriftliche Anweisung, die bei Gefahr im Verzug erteilt wurde, ist innerhalb von 24 Stunden dem örtlich und sachlich zuständigen Richter vorzulegen. Der Richter fällt seine Entscheidungen spätestens innerhalb von 48 Stunden. Ist diese Frist verstrichen oder verwirft der Richter den Antrag, so wird die Maßnahme sofort aufgehoben. In diesem Fall sind Aufnahmen von Abhörinhalten spätestens innerhalb von zehn Tagen vernichtet. Dies wird mit einem Protokoll festgehalten und das Protokoll wird aufbewahrt, um bei Kontrollen vorgelegt werden zu können. Diese Schritte werden von der Stelle, die entsprechend dem Zusatzparagraphen 7 Abs. 10 des Gesetzes über Aufgaben und Befugnisse der Polizei vom 04.07.1934 mit der Nr. 2559 gegründet wurde, in die Wege geleitet. Telekommunikationsüberwachungen, die nach § 135 des Gesetzes Nr. 5271 vorzunehmen sind, werden ebenfalls von diesen Stellen durchgeführt.

(Eingefügter zweiter Absatz am 27.03.2015 durch § 6 des Gesetzes mir Nr. 6638) Der örtlich und sachlich zuständiger Richter ist ein Mitglied des Gerichtes für schwere Straftaten in Ankara.

Im Beschluss oder der schriftlichen Anweisung sind die Personalien der von der Maßnahme betroffenen Person, die Art ihres Telekommunikationsmittels, die von ihr benutzten Telefonnummern oder andere bestimmbare Codes, die die Feststellung ihrer Telekommunikation ermöglichen würden, die Art, die Reichweite, die Dauer der Maßnahme sowie die Gründe fürs Ergreifen dieser Maßnahme anzugeben. Die Entscheidungen dürfen für höchstens drei Monate getroffen werden. Diese Frist darf im Wege desselben Verfahrens jeweils für weitere drei Monate und höchstens dreimal verlängert werden. Allerdings darf der Richter die Frist jeweils um weitere drei Monate wiederholt verlängern, wenn dies aufgrund der Gefahren, die sich aus den fortdauernden Terroraktivitäten ergeben, für erforderlich gehalten wird.

Wird die ergriffene Maßnahme beendet, so werden die Inhalte des Abhörens spätestens innerhalb von zehn Tagen vernichtet. Dies wird mit einem Protokoll festgehalten und das Protokoll wird aufbewahrt, um bei Kontrollen vorgelegt werden zu können.

Im Rahmen der nachrichtendienstlichen Tätigkeiten darf zur Vorbeugung der in diesem Paragraphen genannten Straftaten und durch einen richterlichen Beschluss eine Beobachtung durch technische Mittel vorgenommen werden. Außerdem dürfen bei den öffentlichen Körperschaften und Anstalten sowie Einrichtungen, die öffentliche Dienste anbieten, für den dienstlichen Gebrauch unter Angabe von Gründen schriftlich benötigte Informationen und Dokumente angefragt werden. Geben diese Körperschaften und Anstalten-Einrichtungen aus gesetzlichen Gründen oder Gründen der Geschäftsgeheimnisse die betreffenden Informationen und Dokumente nicht heraus, so dürfen diese nur durch einen richterlichen Beschluss herangezogen werden.

Aufnahmen, die im Rahmen der nach diesem Paragraphen durchgeführten Maßnahmen erlangt werden, dürfen außer zu den in diesem Paragraphen genannten Zwecken nicht verwendet werden. Für die Aufbewahrung und den Schutz der erlangten Informationen gilt das Geheimhaltungsprinzip. Gegen die Personen, die gegen Bestimmungen dieses Absatzes verstoßen haben, dürfen Strafermittlungen unmittelbar von Staatsanwälten durchgeführt

---

[145] Diese Straftaten sind nach § 1 Abs. 6 des Änderungsgesetzes vom 21.02.2016 mit der Nr. 6526 folgende des türkischen Strafgesetzbuchs: a) im Rahmen einer kriminellen Organisation begangene Herstellung und Handel mit Betäubungsmitteln und Geldwäsche, b) im Rahmen einer kriminellen Organisation zum Zwecke der Erlangung illegalen Profits mit Nötigung und Bedrohung begangegene Straftaten, c) im zweiten Buch des vierten Teils der vierten, fünften, sechsten und siebten Abschnitten definierte Straftaten (Paragraphen 305, 318, 319, 323, 324, 325 und 332 ausgenommen).

werden, auch wenn die Verstöße während des Dienstes oder aufgrund des Dienstes begangen wurden.

Der richterliche Beschluss und die schriftliche Anweisung werden von Bediensteten des Nachrichtenpräsidiums der Gendarmerie umgesetzt. Das Datum und die Uhrzeit des Beginns sowie des Endes der Maßnahme sowie die Personalien der ausführenden Person sind in einem Protokoll festzuhalten.

(Geänderter achter Absatz vom 27.03.2015 durch den § 6 des Gesetzes Nr. 6638) Die nach diesem Paragraph durchgeführten Maßnahmen werden durch die behördlichen Vorgesetzen nach ihren Rangverhältnissen, die Vorgesetzen der jeweiligen Verwaltungseinheit, des Stabschefsamts der Gendarmerie und das Inspektionspersonal des betreffenden Ministeriums jährlich mindestens einmal kontrolliert. Diese Maßnahmen dürfen auch von den durch das Präsidialamt beauftragten Aufsichtspersonen kontrolliert werden. Die Ergebnisse der in diesem Rahmen getätigten Kontrollen werden durch einen Bericht dem Sicherheits- und Nachrichtendienstausschuss der Türkischen Nationalversammlung vorgelegt.

Abhörmaßnahmen, die entgegen die in diesem Paragraphen bestimmten Verfahren und Grundsätze durchgeführt werden, sind rechtsunwirksam, und auf die Personen, die in der Weise Abhörmaßnahmen getätigt haben, ist das türkische Strafgesetzbuch vom 26.09.2004 mit der Nr. 5237 anzuwenden.

Verfahren und Grundsätze, die die Anwendung dieses Paragraphs betreffen, sind durch eine vom Staatspräsidenten zu erlassende Rechtsverordnung zu regeln.

Auszüge aus dem Präsidialdekret Nr. 1

Präsidium der Kommission zur Ermittlung von Finanzkriminalität

§ 231 – (Geändert am 07.08.2019 durch § 17 des Präsidialdekrets 43)

(1) Die Kommission zur Ermittlung von Finanzkriminalität untersteht unmittelbar dem Minister und hat folgende Befugnisse:

a) zum Zwecke der Vorbeugung der Geldwäsche und der Terrorismusfinanzierung den Vorbereitungs- und Entwicklungsprozessen hinsichtlich der Planung, der Verfassung der Leitlinien, der Politik und der Strategien beizutragen und zwischen den Körperschaften und Anstalten die Koordination einschließlich der Zusammenarbeit für landesweite Risikoauswertungen zu gewährleisten,

b) in Hinblick auf ihren Tätigkeitsbereich legislative Vorbereitungsdienste vorzunehmen,

c) im Rahmen der Aufdeckung der Risiken der Geldwäsche, der Terrorismusfinanzierung und der Wirtschaftssicherheit und deren Vorbeugung Entwicklungen zu beobachten, Vorbeugungsmaßnahmen zu entwickeln, Analyse, Recherchen und Untersuchungen vorzunehmen

ç) im Rahmen der Vorbeugung der Geldwäsche und der Terrorismusfinanzierung Angaben zu sammeln, Meldungen hinsichtlich der verdächtigen Transaktionen aufzunehmen, diese zu analysieren, zu speichern, nachrichtendienstliche Informationen zu generieren und, wenn für erforderlich erachtet, die betreffenden Einheiten von den generierten Informationen und Analysen zu benachrichtigen,

d) im Hinblick auf das Gesetz vom 11.10.2006 mit der Nr. 5549 über die Verschleierung der Straftaterträgen, die entsprechenden Regelwerke sowie dieses Präsidialdekrets Analysen, Recherchen und Untersuchungen vorzunehmen oder vornehmen zu lassen,

e) einen Sachverhalt der Staatsanwaltschaft mitzuteilen, wenn ernsthafte Verdachtsmomente vorliegen, dass Geldwäsche oder Terrorismusfinanzierung begangen wurde,

f) bei der Staatsanwaltschaft Strafanzeige zum Zwecke der Durchführung erforderlicher Maßnahmen nach der Strafprozessordnung Nr. 5271 zu erstatten, wenn infolge der vorgenommenen Analysen, Recherchen und Untersuchungen Tatsachen dahingehend festgestellt wurden, dass Geldwäsche oder Terrorismusfinanzierung begangen wurde,

g) Sachverhalte, die von der Staatsanwaltschaft, einem Richter oder einem Gericht bezüglich der Geldwäsche oder Terrorismusfinanzierung vorgelegt wurden, zu analysieren und zu untersuchen,

ğ) während des Analyse-, Recherche- und Untersuchungsverfahrens erforderlichenfalls die Polizeibehörde oder andere Einheiten für die Durchführung einer Untersuchung oder Recherche in ihren jeweiligen Aufgabenbereich zu ersuchen,

h) zur Vorbeugung der Geldwäsche oder der Terrorismusfinanzierung mit den nachrichtendienstlichen sowie polizeibehördlichen Einheiten zusammenzuarbeiten und Informationen auszutauschen,

ı) im Rahmen der Vorbeugung der Geldwäsche oder der Terrorismusfinanzierung die Risikokategorien festzustellen und erforderlichenfalls die Meldepflichtigen darüber zu informieren,

i) im Rahmen des Gesetzes Nr. 5549 sowie der entsprechenden Regelwerke die Aufsicht über die Meldepflichtigen vorzunehmen oder vornehmen zu lassen,

j) im Einklang mit dem Gegenseitigkeitsgrundsatz die Aufsicht sowie die Informationsanforderungen der nach den Gesetzen fremder Länder zuständigen Instanzen zu genehmigen, wenn es um die sich in der Türkei befindlichen Einheiten der Meldepflichtigen geht, deren Hauptsitz im Ausland ist,

k) erforderlichenfalls die Aufsicht und Informationsanforderungen bei den sich im Ausland befindlichen Einheiten der Meldepflichtigen vorzunehmen, deren Hauptsitz in der Türkei ist,

l) in Angelegenheiten, die in den Aufgabenbereich fallen, internationale Beziehungen zu pflegen, Informationen und Bewertungen mit den entsprechenden ausländischen Stellen auszutauschen und diesbezüglich Absichtserklärungen zu unterzeichnen, die keinen völkerrechtlicher Vertrag darstellen,

m) bei den Körperschaften und Anstalten des öffentlichen Rechts, natürlichen und juristischen Personen sowie Verbänden ohne juristische Persönlichkeit Dokumente und Informationen aller Art einzufordern,

n) vorläufige Abordnungen der Bediensteten anderer Körperschaften und Anstalten des öffentlichen Rechts ans Präsidium zu ersuchen, wenn deren Kenntnisse und Fachkunde für erforderlich erachtet werden,

o) Aktivitäten zu organisieren, die die Aufmerksamkeit der Allgemeinheit sowie deren Unterstützung fördern würden,

ö) die vom Minister übertragenen anderweitigen Aufträge zu erfüllen.

(2) Die Einheit, die vom Präsidium nach Abs. 1 lit. ğ ersucht wurde, muss das Erforderliche für das Ersuchte umgehend vornehmen,

....

Auszüge aus der tStPO

§ 47. Zeugnis über Erkenntnisse, die als Staatsgeheimnis anzusehen sind

(1) Erkenntnisse über die Tatsache einer Straftat dürfen nicht vor dem Gericht als Staatsgeheimnisse geheim gehalten werden. Erkenntnisse, deren Offenlegung die Auslandsbeziehungen des Staates, seine nationale Verteidigung oder seine nationale Sicherheit beeinträchtigen oder die verfassungsmäßige Ordnung oder Auslandsbeziehungen gefährden können, gelten als Staatsgeheimnisse.

(2) Sind Erkenntnisse, die als Staatsgeheimnis anzusehen sind, Gegenstand eines Zeugnisses, so wird der Zeuge allein von einem Richter des Gerichts oder vom Richterkollegium auch unter Ausschluss des Urkundsbeamten angehört. Der Richter oder der Gerichtsvorsitzende lässt im Nachhinein von diesen Zeugenaussagen lediglich die Erkenntnisse in ein Protokoll aufnehmen, die ihrer Natur nach imstande sind, zur Aufklärung der angelasteten Straftat beizutragen.

(3) Die Bestimmungen dieses Paragraphen werden bei den Straftaten ange-wendet, die mit einer Haftstrafe von mindestens fünf oder mehr Jahren bedroht sind.

(4) Handelt es sich um das Zeugnis des Präsidenten der Republik, so entscheidet er selbst über die Eigenschaft als Geheimnis und darüber, ob er es dem Gericht mitteilt.

§ 125. Durchsicht von Dokumenten durch das Gericht, die als Staatsgeheimnis anzusehen sind

(1) Dokumente, die Erkenntnisse über die Tatsache einer Straftat enthalten, dürfen vor dem Gericht nicht als Staatsgeheimnis geheim gehalten werden.

(2) Dokumente, die Erkenntnisse enthalten, die als Staatgeheimnis anzusehen sind, dürfen nur von einem Richter des Gerichts oder vom Gericht durchgesehen werden. Lediglich die Erkenntnisse, die in diesen Dokumenten enthalten sind und ihrer Natur nach imstande sind, zur Aufklärung der zur Last gelegten Straftat beizutragen, werden vom Richter oder Vorsitzenden des Gerichts in ein Protokoll aufgenommen.

(3) Die Bestimmung dieses Paragraphen ist auf Straftaten anwendbar, die im Mindestmaß mit einer Haftstrafe von fünf oder mehr Jahren bedroht sind.

§ 161. Pflichten und Befugnisse des Staatsanwalts

(1) Der Staatsanwalt kann jede Art der Ermittlung unmittelbar oder durch die ihm unterstellten Beamten der Kriminalpolizei vornehmen; er kann zur Erlangung der im obigen Paragraphen genannten Ergebnisse von allen öffentlichen Bediensteten jegliche Art von Auskunft verlangen. Ergibt sich die Notwendigkeit, dass der Staatsanwalt eine Maßnahme außerhalb des Gerichtsbezirks vornehmen muss, in dem er tätig ist, so ersucht er den örtlichen Staatsanwalt um die Vornahme der betreffenden Maßnahme.

(2) Die Beamten der Kriminalpolizei sind verpflichtet, die von ihnen erfassten Sachverhalte, die festgenommenen Personen sowie die vorgenommenen Maßnahmen dem Staatsanwalt, in dessen Auftrag sie tätig sind, sofort mitzuteilen. Sie haben alle Weisungen dieses Staatsanwalts in Justizangelegenheiten unverzüglich auszuführen.

…

§ 332. Auskunftsverlangen

(1) Auskünfte, die vom Staatsanwalt, Richter oder Gericht im Ermittlungs- oder Hauptverfahren wegen Straftaten schriftlich verlangt werden, sind innerhalb von zehn Tagen zu erteilen. Ist die Erteilung von verlangten Auskünften binnen dieser Frist unmöglich, so sind in derselben Frist der Grund dafür und das Datum mitzuteilen, das für die Erteilung spätestens vorgesehen wird.

…

Nachrichtendienste und Verbrechensbekämpfung in Ungarn

Ágota Margit Szabóné

I. Einleitung

In Ungarn als ehemaligem Ostblockstaat ist die Tätigkeit der nationalen Sicherheitsdienste ein heikles Thema. Vor 1990 war die Aufklärung – die Tätigkeit der Geheimdienste – nicht einmal gesetzlich geregelt,[1] und die Dienste waren aufgrund der Unvorhersehbarkeit und Unberechenbarkeit ihrer Aktivitäten berüchtigt und gefürchtet. Vor dem Hintergrund der mit dem Systemwechsel gesetzlich deklarierten Rechtsstaatlichkeit mussten die Behörden, die für das alte Regime standen, neu organisiert werden. Ein gänzlicher Verzicht kam trotz des schlechten Rufes der Geheimdienste nicht in Betracht, weil die Informationen, die nur durch solche Dienste beschafft werden können, auch von der Regierung eines demokratischen Rechtsstaates nicht entbehrt werden können. Um die öffentliche Sicherheit, die ein Wesensmerkmal des Staates ist, aufrechtzuerhalten, muss der Staat imstande sein, bestimmte Rechtsgüter zu schützen und auf Bedrohungen schnell und effektiv zu reagieren, dazu ist er auf entsprechende Informationen angewiesen.[2]

Die Nachrichtendienste sind also auch im demokratischen Rechtsstaat Ungarn nicht verschwunden, aber seit 1990 nun gesetzlich geregelt. Ihre Tätigkeiten wurden der neuen Rechtsordnung angepasst, sodass diese und ihre Existenz nicht mehr dem Prinzip der Rechtsstaatlichkeit widersprechen. Das Gesetz von höchstem Rang, das ungarische Grundgesetz, bestimmt ihre wichtigste Aufgabe, die dem Wortlaut nach die Bewahrung der Unabhängigkeit und der Rechtsordnung Ungarns ist. Außerdem sind sie der einschlägigen Vorschrift zufolge für die Durchsetzung der nationalen Sicherheitsinteressen verantwortlich.[3] Die Bestimmungen des Grundgesetzes bezüglich der Organisation, Rechtsstellung, Befugnisse und des Verfahrens der Nachrichtendienste sind in dem mehrmals geänderten Zweidrittelgesetz Nr. CXXV aus dem Jahre 1995 (im Folgenden: Nbtv genannt)[4] konkretisiert.

Die Grundnormen der Strafverfolgung – die wichtigsten Garantien im Strafverfahren und die Bestimmungen zu den Strafverfolgungsbehörden – sind ebenfalls im ungarischen Grundgesetz zu finden. Den Verlauf des Strafverfahrens regelt die ungarische Strafprozessordnung, deren aktuell gültige Version am 1. Juli 2018[5] in Kraft trat. Mit ihr bekam die strafprozessuale Informationsbeschaffung völlig neue Rechtsgrundlagen, die Ziele und Funktionen der geheimen Informationssammlung wurden neu bestimmt.[6]

---

[1] Finszter Géza/Korinek László: Az eltűnt gyanú nyomában *(in: Belügyi Szemle 2018/3)*.

[2] Vida Csaba: A nemzetbiztonsági tevékenység szerepe a társadalomban *(in: 10.17047/HADTUD.2015.25.E.221)*.

[3] Art. 46 des ungarischen Grundgesetzes (uGG).

[4] Gesetz über die nationalen Sicherheitsdiensten (Nbtv.).

[5] Gesetz Nr. XC über das Strafverfahren (uStPO).

[6] Mészáros Bence: A bűnügyi hírszerzés új rendszere hazánkban.

Eins der wichtigsten Nova des neuen Gesetzes ist die Einführung des Vorbereitungsverfahrens vor dem offiziellen Ermittlungsverfahren. Der uStPO zufolge ist es der Zweck des Vorbereitungsverfahrens, das Bestehen oder Nichtbestehen des Anfangsverdachts einer Straftat zu überprüfen.[7] Im Rahmen des Vorbereitungsverfahrens werden die noch fehlenden Informationen beschafft, aufgrund derer die Entscheidung über die Notwendigkeit der Eröffnung des Ermittlungsverfahrens getroffen werden kann. Für das Vorbereitungsverfahren sind die Vorschriften des Ermittlungsverfahrens anzuwenden.[8] Problematisch ist das neue Vorbereitungsverfahren nach einigen Stimmen in der Literatur deswegen, weil der Gesetzgeber dadurch bereits in dieser Phase des Strafverfahrens, in der der anfängliche Verdacht kaum substantiiert ist (genannt „Verdacht des Verdachtes"), den Weg zur Anwendung von geheimdienstlichen Methoden – u.a. zur geheimen Informationssammlung – öffnet.[9]

In der neuen Strafprozessordnung ist ein ganzes Kapitel der geheimen Informationssammlung – im neuen Gesetz „verdeckte (Ermittlungs)mittel" genannt – gewidmet.

Sowohl die Möglichkeit, im Rahmen des Vorbereitungsverfahrens geheim Informationen zu sammeln, als auch das Bestehen eines eigenen Kapitels weisen darauf hin, dass in der Zukunft geheimen Ermittlungen größere Bedeutung als den klassischen, offenen Ermittlungsmethoden zukommt. Ob dieser gesetzgeberische Wille auch in der Praxis auf fruchtbaren Boden trifft, wird sich erst mit der Zeit zeigen, da seit dem Inkrafttreten des neuen Gesetzes nur eine relativ kurze Zeitspanne verstrichen ist und sich bisher landesweit kaum eine homogene Praxis ausformen konnte.

Zusammenfassend kann also gesagt werden, dass aufgrund der gesetzlichen Regelung in Ungarn erste Ansätze zu einer gewissen organisatorischen und funktionalen Trennung zwischen den Nachrichtendiensten und den Strafverfolgungsbehörden vorhanden sind. Wieweit diese Trennung reicht und inwiefern sich die Tätigkeiten der Nachrichtendienste und der Strafverfolgungsbehörden überschneiden, lässt sich erst nach einer Darstellung der beiden Bereiche in ihren Grundzügen beantworten.

II. Die Nachrichtendienste in Ungarn

A. Die Nachrichtendienste im Allgemeinen

Das ungarische Gesetz benutzt den Sammelbegriff „nationaler Sicherheitsdienst" für die fünf Organisationen, die sich mittels geheimdienstlicher Methoden mit

---

[7] § 340, Abs. 1 uStPO.

[8] § 344, Abs. 7 uStPO.

[9] Finszter Géza/Korinek László: Az eltűnt gyanú nyomában (*in: Belügyi Szemle, 2018/3)*.

Informationsbeschaffung und Abwehr von Gefahren befassen.[10] Unter den zur Zeit fungierenden Diensten – die im Folgenden näher beschrieben werden – ist ein Dienst für die militärische Aufklärung zuständig, während die vier anderen zivile Einheiten sind.

Nach Csaba Vida sind die Nachrichtendienste Dienstleistungsorgane der Regierung und versorgen diese mit Informationen .[11] Dies spiegelt sich auch im Gesetz wider. Laut § 2 Nbtv. stehen alle fünf Dienste unter der Leitung der Regierung. Jeder Dienst verfügt über ein eigenes Budget und ist in seinem gesetzlich festgelegten Aufgabenbereich landesweit zuständig. Nach § 10 Nbtv. leitet die Regierung alle fünf Nachrichtendienste durch jeweils einen im Gesetz bestimmten Minister, der u.a. bezüglich des ihm unterstehenden Nachrichtendienstes weisungsberechtigt ist. Der Minister ist auch für die Durchführung der Kontrolle zuständig, die das zweck- und gesetzmäßige Funktionieren des jeweiligen Dienstes gewährleisten soll.

Die Nachrichtendienste in Ungarn unterliegen darüber hinaus einer parlamentarischen Kontrolle, § 14 Nbtv. Diese wird durch einen Ausschuss des Parlaments ausgeübt, dessen Vorsitzender immer ein Abgeordneter der Oppositionspartei ist.

B. Das Informationsamt (Információs Hivatal)

Diese Behörde ist der zivile Auslandnachrichtendienst Ungarns, so versteht sie sich auf der offiziellen Webseite.[12] Sie existiert als selbständiger Dienst seit dem 1. März 1990 und untersteht zurzeit dem Minister für Ausländerwesen.

Die Behörde beschafft, analysiert, bewertet und leitet auslandsbezogene Informationen weiter, die für die Entscheidungen der Regierung nötig sind und das Interesse der Sicherheit des Staates tangieren können. Hierzu gehört auch die Sammlung von Informationen, die für die Bekämpfung des internationalen Terrorismus und der organisierten Kriminalität benötigt werden. Damit ergibt sich die erste Überschneidung zwischen der nachrichtendienstlichen Informationssammlung und der Strafverfolgung, indem das ungarische Informationsamt die Aufgabe hat, Informationen über zwei wichtige Kriminalitätsfelder zu sammeln. Zwar ist der Zweck der Informationssammlung hier die Beratung der Regierung und nicht die Förderung der Strafverfolgung, dessen ungeachtet ist nicht von der Hand zu weisen, dass die gesammelten Informationen Auswirkungen auf die Strafverfolgung entfalten können, auf die im Zusammenhang mit Ausführungen zur informationellen Trennung der Nachrichtendienste von den Strafverfolgungsorgane noch einzugehen ist (unten IV.D).

---

[10] Vida Csaba: A nemzetbiztonsági tevékenység szerepe a társadalomban (*in: 10.17047/HADTUD.2015.25.E.221)*.

[11] Vida Csaba: A nemzetbiztonsági tevékenység szerepe a társadalomban (*in: 10.17047/HADTUD.2015.25.E.221)*.

[12] www.mkih.hu/Rólunk.

Außerdem klärt das Informationsamt Bestrebungen und Tätigkeiten von ausländischen Nachrichtendiensten auf, die die Unabhängigkeit Ungarns bzw. politische, wirtschaftliche oder andere erhebliche Interessen des Staates verletzen oder gefährden.[13] Schließlich ist das Amt für die Sicherheit der aus Sicht der Regierung wichtigen ungarischen Institutionen im Ausland verantwortlich.

Dieser Dienst ist mit klassischen nachrichtendienstlichen Befugnissen ausgestattet, die sich auf die Beschaffung von Informationen und die Aufklärung beschränken. Mit anderen Worten ist das Informationsamt nur berechtigt, mithilfe geheimdienstlicher Methoden Informationen zu beschaffen.

C. Das Amt für Verfassungsschutz (Alkotmányvédelmi Hivatal)

Zu den Vorgängern dieses Dienstes gehörte u.a. das gefürchtete III/III Gruppenkommando, das für die innere Sicherheit des Ungarns bzw. für die Abwehr von inneren Gefahren zuständig war. Bis 2010 hieß die Behörde Nationales Sicherheitsamt (Nemzetbiztonsági Hivatal). Später wurde der Name des zivilen Sicherheitsdienstes von Ungarn in Amt für Verfassungsschutz geändert. Der ungarische Verfassungsschutz untersteht dem Innenminister.

Der Verfassungsschutz hat über die Aufklärungskompetenzen hinausgehend auch Abwehrbefugnisse (Spionageabwehr, Gefahrenabwehr) bezüglich eines Teils seiner im Nbtv. bestimmten Aufgaben. Zu den Tätigkeiten dieses Dienstes gehören u.a. Spionageabwehr, Verfassungsschutz, Schutz der Staats- bzw. Wirtschaftssicherheit, Überprüfung von bestimmten Personen aus Gründen der Staatssicherheit und Mitwirkung in Migrations- und Einbürgerungsverfahren.[14] Unter Verfassungsschutz ist die Aufklärung und Abwehr von verdeckten Bestrebungen, die die verfassungsmäßige Ordnung in Ungarn rechtswidrig zu beeinträchtigen beabsichtigen, zu verstehen.

Nach § 5. Nbtv. ist das Amt befugt, bestimmte Straftaten – wie z.B. Straftaten gegen den Staat – bis zur Einleitung des Ermittlungsverfahrens aufzuklären, sowie Informationen über im Gesetz abschließend aufgezählte Delikte – z.B. das Herbeiführen von öffentlicher Gefahr – zu sammeln. Laut der offiziellen Webseite des Verfassungsschutzes gehört zu den Partnerorganen dieses Sicherheitsdienstes neben den anderen Sicherheitsdiensten auch die Terror-Abwehr-Einheit der Polizei.[15]

Im Vergleich zum ungarischen Auslandsnachrichtendienst ist der Verfassungsschutz in deutlich mehr Kriminalitätsfeldern informationssammelnd tätig. Gleich-

---

[13] § 4 Nbtv.

[14] www.ah.gov.hu/Feladataink.

[15] www.ah.gov.hu/Társszervek.

zeitig markiert die Einleitung des Ermittlungsverfahrens die gesetzliche Grenze, ab der der Verfassungsschutz keine Informationen über bestimmte Straftaten mehr sammeln soll. Allerdings ist diese Grenzsetzung in § 5 Nbtv missverständlich. Denn Informationsinteressen des Verfassungsschutzes über bestimmte Sachverhalte können auch nach der Einleitung eines Ermittlungsverfahrens fortbestehen. Es spricht nichts dagegen, dass die Aufklärung ein und desselben Sachverhalts sowohl für den Verfassungsschutz und als auch für die Strafverfolgungsbehörde erforderlich ist. Es liegt jedoch auf der Hand, dass die Aufklärung beider Behörden verschiedenartig ist und sie unterschiedliche Zwecke verfolgen. Aus diesem Grund ist § 5 NbtV so zu verstehen, dass der Verfassungsschutz nach der Einleitung des Ermittlungsverfahrens wegen eines Sachverhalts *keine Aufklärung für die Strafverfolgung* betreiben darf. Gleichzeitig ist darauf hinzuweisen, dass das Amt für Verfassungsschutz sowohl informationell als auch organisatorisch eine gewisse Verbindung zur Strafverfolgung hat. Denn der ungarische Verfassungsschutz sammelt immerhin Informationen über einige wichtige Kriminalitätsfelder. Eine durchgehende Übermittlung von strafverfolgungsrelevanten Informationen durch das Amt an die Strafverfolgungsbehörden würde heißen, dass es keine informationelle Trennung zwischen dem Verfassungsschutz und der Strafverfolgung gibt. Auch organisatorisch ist es angebracht, darauf hinzuweisen, dass das Amt mit der Polizei zusammenarbeitet. Auf die Frage, wie diese Umstände zu bewerten sind, wird im Folgenden noch gesondert eingegangen (IV.A. und D.)

D. Der Fachdienst für Staatssicherheit (Nemzetbiztonsági Szakszolgálat)

Der Fachdienst für Staatssicherheit[16] Ungarns ist im Jahre 1996 vom Nationalen Sicherheitsamt (ehemaliger Verfassungsschutz) abgetrennt worden. Seitdem fungiert er als ein selbständiges Organ, dessen Grundfunktion die Leistung bestimmter Fachdienste ist. Auch der Fachdienst untersteht dem Innenminister.

Die Behörde bedient die Staatssicherheits- und Strafverfolgungsorgane, die gesetzlich ermächtigt sind, die Dienstleistungen des Fachdienstes zu beantragen. Mithilfe ihres hochgebildeten Fachpersonals und der permanent weiterentwickelten Mittel und Methoden sammelt oder beschafft der Fachdienst Informationen. Auch als Fachexpertenstelle wird der Dienst in Anspruch genommen.[17] Dadurch unterstützt er den Staatssicherheitsschutz und trägt zur Prävention und Aufdeckung von Straftaten sowie zur Effektivität der Rechtsprechung bei. In der Regel werden sowohl nachrichtendienstliche geheime Informationssammlungen als auch die verdeckten Ermittlungen im Strafverfahren mithilfe dieses Dienstes ausgeführt. Hierzu gehören

---

[16] Die deutsche Benennung der Behörde laut Gründungsstatut des Dienstes.

[17] www.nbsz.hu/Tevékenység, működés.

insbesondere die Telekommunikationsüberwachungen aller Art, die unter dem gemeinsamen Dach des Fachdienstes durchgeführt werden. Ob und wieweit dieser Umstand den Gedanken einer gewissen informationellen Trennung zwischen den Sicherheitsdiensten durchbricht, ist nicht geklärt. Ein Schutz vor der Zweckentfremdung der gesammelten Informationen ist dennoch gesetzlich verankert. Nach § 8 Abs. 2 Nbtv. ist es dem Fachdienst untersagt, die Regierung über die Ergebnisse der Verfahren und über die gesammelten Informationen selbst zu unterrichten.

Es gibt zurzeit insgesamt acht Behörden, die beim Fachdienst die Inanspruchnahme von geheimen Mitteln und Methoden beantragen dürfen. Diese sind gesetzlich abschließend geregelt. Folgende Behörden sind antragsberechtigt:

- die Einheit der Polizei, die für die allgemeinen polizeilichen Aufgaben verantwortlich ist,
- die innere Kontrolleinheit der Polizei,
- die Terror-Abwehr-Einheit der Polizei,
- das Nationale Steuer- und Zollamt,
- die Staatsanwaltschaft,
- das Informationsamt,
- das Amt für Verfassungsschutz und
- der Militärische Staatssicherheitsdienst.

Teilweise ist die Behörde ermächtigt, ihre geheimen Mittel auch auf eigene Initiative – bei der Ausübung einzelner im Gesetz bestimmter Aufgaben, wie z.B. bei der Überprüfung von bestimmten Personen aus Gründen der nationalen Sicherheit – in Anspruch zu nehmen.

E. Anti-Terror-Informations-und-Analysezentrum (Terrorelhárítási Információs és Bűnügyi Elemző Központ, TIBEK)

Das Anti-Terror-Informations-und-Analysezentrum (TIBEK)[18] ist als jüngster Dienst seit dem 17. Juli 2016 tätig. Auch dieses untersteht dem Innenminister.

Das Zentrum wurde vor dem Hintergrund gegründet, dass der internationale Terrorismus eine große Herausforderung für die Sicherheit der Staaten darstellt. Er bedroht die Schutzfunktion des Staates in einer besonderen Weise. Es bedarf deshalb effektiver Gegenmaßnahmen, die die Freiheit, Sicherheit und Ordnung sichern. Dazu ist eine kohärente Organisation nötig, die im Besitz der erforderlichen Informationen und des diesbezüglichen Wissens ist und auch die Kompetenz hat, zu handeln.[19]

---

[18] Die deutsche Benennung der Behörde laut Gründungsstatut des Dienstes.

[19] www.tibek.gov.hu/Bemutatkozás.

Das Zentrum fungiert als oberste Sammel- und Verteilungsstelle von relevanten Informationen. Es steht mit seinen Diensten der Polizei, den anderen nationalen Sicherheitsdiensten und Organisationen der öffentlichen Verwaltung, die auf störende Faktoren im Bereich öffentlicher und nationaler Sicherheit zu reagieren haben, zur Verfügung.

Der Auftrag der Behörde ist in § 8/A Nbtv. normiert. Nach dieser Vorschrift bewertet die Behörde die beschaffenen Informationen, koordiniert und fördert die Informationsgewinnungsprozesse, die von anderen Organen geführt werden. Auch analysiert die Behörde permanent die Sicherheits- und die Kriminalitätslage Ungarns, unterrichtet die Regierung und macht Vorschläge für deren Entscheidungen. Die Behörde analysiert und bewertet die erhobenen Informationen und koordiniert und fördert die Informationsgewinnungsprozesse, die von anderen Organen durchgeführt werden. Sollten die erhobenen Informationen den Verdacht einer Straftat begründen, so ist das Analysezentrum verpflichtet, bei der zuständigen Ermittlungsbehörde Strafanzeige zu erstatten.

Diese gesetzlich normierte Pflicht zeigt einerseits, dass das Anti-Terror-Informations-und-Analysezentrum keine unmittelbare Strafverfolgung betreibt. Andererseits impliziert die genannte Pflicht, dass man sich erhofft, aufgrund der Auswertungs- und Analystätigkeiten des Zentrums strafverfolgungsrelevante Verdachtsmomente abzuschöpfen. Insofern unterstützt das Zentrum auch die Strafverfolgung.

Das Zentrum fungiert auch als eine Art Datenbank, die die relevanten Informationen sowohl für die Ermittlungsbehörden als auch für die anderen Nachrichtendienste und für die Regierung zugänglich macht. Das Zentrum leitet die Informationen an die jeweiligen Auftraggeber weiter. Die Behörden, die berechtigt sind, an das Zentrum Anträge zu stellen, sind in § 30/A Nbtv. aufgelistet, aber auch die offizielle Webseite der Behörde weist auf die kooperierenden Organen hin.[20] Péter Nyeste fasst die Funktion des Analysezentrums folgenderweise zusammen: Als Nachrichtenfusionszentrum ist das TIBEK wie ein Verbindungskanal, der die Nachrichtenbedürfnisse der Regierung entweder befriedigt oder an die übrigen Nachrichtendienste weiterleitet, und gleichzeitig die kooperierenden Organe verbindet und diese unterrichtet.[21] Wie diese Ausführungen zeigen, spielt der Gedanke einer gewissen informationellen Trennung zwischen den Sicherheitsbehörden bei der Aufgaben- und Befugniszuweisung des Anti-Terror-Informations-und-Analysezentrums kaum eine Rolle. Im Gegenteil, es geht darum, in diesem wichtigen Bereich schwerer Kriminalität u.a. den Informationsaustausch zwischen den Diensten zu fördern.

---

[20] www.tibek.gov.hu/Együttműködő szervek.

[21] Nyeste Péter: A titkos információgyűjtés és a leplezett eszközök, a felderítés új modellje *in*: Belügyi Szemle, 2018/5.

F. Der nationale Sicherheitsdienst für Militärwesen (Katonai Nemzetbiztonsági Szolgálat)

Unter den ungarischen Nachrichtendiensten ist der nationale Sicherheitsdienst für Militärwesen der einzig militärische. Er ist als Ergebnis der Fusion von zwei unabhängigen Anstalten, die sich mit der Informationsbeschaffung bzw. der Abwehr von Gefahren befassten, am 1. Januar 2012 zu Stande gekommen. Seit der Integration hat der Dienst Aufgaben auf beiden Gebieten inne. Der Dienst untersteht dem Landesverteidigungsminister.

Die Grundfunktionen dieses Sicherheitsdienstes bestehen darin, die Bestrebungen, die sich gegen die Sicherheit Ungarns richten, aufzudecken und zu verhindern. Außerdem fördert er das Treffen von politischen und militärischen Entscheidungen und die Durchsetzungsfähigkeit von nationalen Interessen. Diese Aufgaben, die sich scheinbar mit denen des Verfassungsschutzes überschneiden, sind vor dem Hintergrund der sachlich unterschiedlichen Zuständigkeitsbereiche zu interpretieren: Der nationale Sicherheitsdienst für Militärwesen garantiert das gesetzmäßige Funktionieren des Landesverteidigungsministeriums und das der ungarischen Streitkräfte. Auch die Unterstützung der Informationsbeschaffung der ungarischen Streitkräfte und die Garantie der Sicherheit der Soldaten, die im Rahmen von internationalen Operationen tätig sind, gehören zu den Grundfunktionen des Dienstes.[22]

Nach § 6 lit g)–i) Nbtv sammelt der Dienst Informationen über Cyber-Tätigkeiten, Cyber-Organisationen, über terroristische Organisationen und über illegalen Waffenhandel, die unter dem Blickwinkel der Landesverteidigung relevant sind, oder die die nationale Sicherheit beeinträchtigen können. So wie es beim Verfassungsschutz der Fall ist, werden auch dieser Behörde bezüglich im Gesetz abschließend genannter Delikte – wie z.B. Verbrechen gegen den Staat, Verbrechen gegen die Menschlichkeit und militärische Delikte – Aufgaben übertragen und Befugnisse eingeräumt. Die Aufklärungskompetenz des nationalen Sicherheitsdienstes für Militärwesen bezüglich dieser Delikte ist begrenzt, wenn die Strafermittlungen eingeleitet sind.

Anders als beim Verfassungsschutz wird aber diesem Dienst Aufklärungskompetenzen bezüglich der terroristischen Handlungen – auch das Unterlassen der Anzeigeerstattung und die Terrorismusfinanzierung – und der Kriegshetze, die in die sachliche Zuständigkeit des Dienstes fallen, ohne die oben genannte Grenze, also nicht nur bis zur Einleitung der Ermittlungen, eingeräumt.[23]

Der Dienst leitet die gesammelten und analysierten Informationen an das Verteidigungsministerium weiter. Wie der gesetzliche Adressat der gesammelten Informationen impliziert, erfolgt die militärische Aufklärung bestimmter Straftaten durch

---

[22] www.knbsz.gov.hu/Köszöntő.

[23] § 6 lit ma)–mb) Nbtv.

den nationalen Sicherheitsdienst für Militärwesen grundsätzlich nicht zum Zwecke einer Strafverfolgung.

III. Die Strafverfolgungsbehörden

A. Das Strafverfahren und die darin handelnden Organe aufgrund der neuen Regelung

Das Strafverfahren unterteilt sich aufgrund der uStPO in Vorbereitungsphase, in Ermittlungsphase – innerhalb welcher Aufklärung und Untersuchung voneinander zu unterscheiden sind – und in gerichtliche Phase. Die Aufklärung ist weniger formal, als die Untersuchung, und hier ist das Ziel in erster Linie die Sammlung und Herbeischaffung von Informationen, während in der Phase der Untersuchung hauptsächlich Beweise beschaffen werden sollen. In der Phase der Untersuchung ist der Tatverdächtige schon bekannt, deshalb geschieht hier die Vorbereitung der Entscheidung bezüglich der Klageerhebung, zu der die nötigen Beweise beschaffen werden sollen.[24]

Die Vorbereitungsphase ist nicht obligatorisch. Das Strafverfahren kann auch gleich mit der Ermittlungsphase beginnen, wenn die zur Verfügung stehenden Informationen zur Begründung eines Anfangsverdachts genügen. Auch die gerichtliche Phase kann entfallen, wenn das Verfahren in der Ermittlungsphase eingestellt wird.

Das Vorbereitungsverfahren als eine Neuerung der neuen Strafprozessordnung soll an dieser Stelle nochmal erwähnt und kurz beschrieben werden. Das Einfügen dieser neuen Phase vor der Einleitung der Ermittlungen wurde für erforderlich erachtet, um die Vorschriften der geheimen Informationssammlung, die vor dem Inkrafttreten der uStPO in mehreren verschiedenen Gesetzen zu finden waren, in die uStPO zu integrieren; diese wurden einheitlich in „verdeckte Ermittlungsmittel“ umbenannt.[25] Die neue Regelung ermöglicht, dass vor der Eröffnung des Ermittlungsverfahrens, aber im Rahmen des Strafverfahrens – im Vorbereitungsverfahren – eine Art Aufklärung stattfindet, deren Zweck die Bestätigung oder der Ausschluss des Anfangverdachtes ist.[26] Zu diesem Zwecke können von nun an auch im Vorbereitungsverfahren, also ohne Anfangsverdacht, verdeckte Ermittlungsmittel – sowohl genehmigungsbedürftige, als auch solche, zu denen keine Genehmigung notwendig ist – angewendet werden.

---

[24] Nyeste Péter: A titkos információgyűjtés és a leplezett eszközök, a felderítés új modellje *in*: Belügyi Szemle 2018/5.

[25] Mészáros Bence: A bűnügyi hírszerzés új rendszere hazánkban.

[26] Nyeste Péter: A titkos információgyűjtés és a leplezett eszközök, a felderítés új modellje *in*: Belügyi Szemle, 2018/5.

In der uStPO sind die Strafverfolgungsbehörden benannt und ihre Befugnisse festgelegt. Laut Gesetz handeln im Strafverfahren die Ermittlungsbehörden, die Staatsanwaltschaft und das Gericht.

B. Die Staatsanwaltschaft

Nach Art. 29 Abs. 1 des ungarischen Grundgesetzes ist ausschließlich die Staatsanwaltschaft befugt, die Strafverfolgungsbedürfnisse des Staates durchzusetzen. Als Anklagebehörde mit neutraler Aufklärungspflicht wirkt sie an der Rechtsprechung mit. Die Unabhängigkeit der Staatsanwaltschaft ist durch diese Vorschrift des Grundgesetzes garantiert. Art. 29 schreibt die grundlegenden Aufgaben der Staatsanwaltschaft vor, die näher in einem anderen Gesetz, im Gesetz Nr. CLXIII aus dem Jahre 201[27] bestimmt werden.

Die Staatsanwaltschaft ermittelt, übt Kontrolle über die Gesetzmäßigkeit der Aufklärung aus und leitet die Untersuchung.[28] Für die Staatsanwaltschaft ist die Aufklärung eine Pflicht, deshalb handelt die Behörde ex officio.

Im Rahmen der Ermittlungskompetenz ist die Staatsanwaltschaft befugt, die Ermittlung in einer beliebigen Strafsache an sich zu ziehen.[29] Außerdem gibt es bestimmte Straftaten – u.a. die Amtsbestechung, oder auch bestimmte Straftaten, die sich z.B. gegen Richter richten oder von Richter begangen wurden –, für deren Ermittlung ex lege ausschließlich die Staatsanwaltschaft zuständig ist.[30]

In der Leitung der Untersuchung ist auch die Befugnis inbegriffen, dass die Staatsanwaltschaft der jeweiligen Ermittlungsbehörde die Weisung erteilen kann, eine bestimmte Ermittlungsmaßnahme durchsetzen zu müssen.[31]

Die Staatsanwaltschaft ist befugt, selbst das Vorbereitungsverfahren durchzuführen. Falls dieses von einer anderen berechtigten Behörde durchgeführt wird, übt sie die Kontrolle über die Gesetzmäßigkeit des Verfahrens aus.[32]

Im Gerichtsverfahren vertritt die Staatsanwaltschaft die Anklage und hat Antragsrecht in jeder Frage, über die das Gericht zu entscheiden hat.[33]

---

[27] Gesetz über die Staatsanwaltschaft (Ütv.).

[28] § 25, Abs. 2 uStPO.

[29] § 26, Abs. 5 uStPO.

[30] § 30 uStPO.

[31] § 26, Abs. 3, lit. b) uStPO.

[32] § 25, Abs. 3 uStPO; § 17., Abs. 1 Ütv.

[33] § 21, Abs. 2., lit a)–b) Ütv.

C. Die Ermittlungsbehörden

Während die Gerichte und die Staatsanwaltschaft zur judikativen Macht gehören, unterstehen die Ermittlungsbehörden der Exekutive. Demzufolge sind sie im Gegensatz zu den oben beschriebenen zwei Organen der Regierung untergeordnet und an die Weisungen der Regierung, des Leiters der jeweiligen Behörde und auch an die der Staatsanwaltschaft gebunden.

Laut uStPO ist die generelle Ermittlungsbehörde die Polizei, genauer gesagt die Einheit der Polizei, die für die Erfüllung der allgemeinen polizeilichen Aufgaben verantwortlich ist.[34] Für die Ermittlung bestimmter Straftaten jedoch, die im Gesetz abschließend aufgelistet sind, ist das Nationale Steuer- und Zollamt zuständig.[35]

Die Vorschriften der uStPO legen die Aufgaben der Ermittlungsbehörden und deren Verhältnis zur Staatsanwaltschaft fest. Demnach sind die Ermittlungsbehörden befugt, zwecks Aufklärung von Straftaten Vorbereitungsverfahren und Ermittlungen durchzuführen. Das Vorbereitungsverfahren und die Aufklärung im Strafverfahren führen die Ermittlungsbehörden selbständig durch, im Untersuchungsverfahren unterstehen sie jedoch der Leitung der Staatsanwaltschaft. Die Ermittlungsbehörden sind befugt, alle Ermittlungsmaßnahmen durchzuführen, die nicht in die Zuständigkeit des Gerichts oder der Staatsanwaltschaft fallen. Die Ermittlungsbehörden haben die Weisungen der Staatsanwaltschaft zu befolgen.[36]

1. Die Polizei

Die Rechtsstellung und die grundlegenden Aufgaben der Polizei sind im ungarischen Grundgesetz, im Artikel 46, festgelegt. Hiernach hat die Polizei die Verhinderung und Aufklärung von Straftaten, den Schutz der öffentlichen Sicherheit und öffentlichen Ordnung sowie den Grenzschutz zur Aufgabe. Die Polizei untersteht dem Innenminister.

Die Bestimmungen des Grundgesetzes bezüglich der Polizei werden in einem Zweidrittelgesetz, nämlich im Gesetz Nr. XXXIV aus dem Jahre 1994 (im Folgenden: Rtv.)[37] konkretisiert. Diesem Gesetz zufolge hat die Polizei nicht nur die Befugnis, die Strafverfolgung bezüglich einzelner Taten, sondern auch eine präventiv/vorbeugende Verbrechensbekämpfung zu betreiben, etwa im Bereich des Terrorismus. Diesbezüglich beschafft, analysiert und übermittelt die Polizei Informationen und klärt dadurch solche Bestrebungen auf, die in die Begehung von Straftaten münden können. Die präventiv gesammelten Informationen übermittelt die Polizei weiter an die Strafverfolgung. Die Vorfeldbekämpfung auf dem Gebiet der

---

[34] § 34, Abs. 1 uStPO.

[35] § 34, Abs. 2 uStPO.

[36] § 31 uStPO.

[37] Gesetz über die Polizei (Rtv.).

Strafverfolgung wird vom Gesetz als kriminalitätsbezogene Informationsbeschaffung definiert, deren Gegenstand nicht eine bestimmte Straftat ist, sondern die Kriminalität im Allgemeinen, die die gesellschaftliche Ordnung von Ungarn gefährdet.[38] Nach Géza Finszter gehört auch die Vorbeugung von Rechtsverletzungen zu den polizeilichen Aufgaben. Diese klassische Überwachungsfunktion der Polizei nennt er „polizeiliche Präsenz".[39] Im Zusammenhang mit der genannten Vorbeugungsbefugnis der Polizei lässt sich die Frage aufwerfen, ob und inwiefern die Vorfeldinformationsbeschaffung der Polizei einer nachrichtendienstlichen Informationsbeschaffung ähnelt. Bejahendenfalls ließe sich argumentieren, dass die ungarische Polizei ihre eigene nachrichtendienstliche Einheit hat. Zu erwähnen ist in diesem Zusammenhang erneut das neue Vorbereitungsverfahren, in dem die Polizei ohne einen Anfangsverdacht auf geheime Methoden zurückgreifen und ermitteln darf. Beides sind sehr wichtige Indizien dafür, dass eine funktionelle Trennung seitens der Polizei nicht streng befolgt wird, denn die Polizei beschränkt sich nicht mehr auf Aufklärung einzelner Taten.

2. Das Nationale Steuer- und Zollamt

Zu dieser Behörde sind im ungarischen Grundgesetz keine Vorschriften zu finden, aber in einem Zweidrittelgesetz, nämlich im Gesetz Nr. CXXII aus dem Jahre 2010,[40] sind die Aufgaben, Rechtstellung und Befugnisse dieser Behörde ausführlich beschrieben.

Das Nationale Steuer- und Zollamt ist eine zentrale Behörde, die der Regierung untersteht. Die Regierung leitet die Behörde durch das Finanzministerium; der Finanzminister hat Weisungsrecht bezüglich des Steueramtes.[41]

Das Nationale Steuer- und Zollamt ist nicht ausschließlich eine Ermittlungsbehörde. Ähnlich wie die Polizei besteht sie aus mehreren Organen, unter denen es auch solche mit Ermittlungskompetenzen gibt. Die Straftaten, für deren Ermittlung das Nationale Steuer- und Zollamt zuständig ist, sind im Gesetz abschließend aufgelistet, genauso wie die Aufgaben der Behörde im Bereich der Prävention von Straftaten und der Strafverfolgung.[42]

---

[38] Nyeste Péter: A titkos információgyűjtés és a leplezett eszközök, a felderítés új modellje *in*: Belügyi Szemle, 2018/5.

[39] Finszter Géza: Közrend-közbiztonság-jogbiztonság (2000–2015) *in:* Biztonsági kihívások a 21. században.

[40] Gesetz über das Nationale Steuer- und Zollamt (NAV tv.).

[41] § 1, Abs. 1 NAV tv.

[42] § 13 NAV tv.

IV. Die Trennung von Nachrichtendiensten und Strafverfolgungsbehörden

Das ungarische Recht kennt ein Prinzip der Trennung zwischen Nachrichtendiensten und Strafverfolgungsbehörden nicht explizit. Der Leitgedanke dieses aus Deutschland stammenden Prinzips lässt sich dennoch in einigen Bestimmungen des ungarischen Rechts aufspüren, soweit es um die normative Reglementierung der Verhältnisse zwischen den Nachrichtendiensten, der Gefahrenabwehr und der Strafverfolgung geht.

A. Organisatorische Trennung

Oben sind die Nachrichtendienste und die Strafverfolgungsbehörden in Ungarn einzeln vorgestellt worden. Die gesetzlichen Bestimmungen, auf die ich mich berufen habe, stellen klar, dass die Nachrichtendienste und die Strafverfolgungsbehörden organisatorisch strikt voneinander getrennt sind, und der Aufbau der einzelnen Organe der beiden Gebiete zeigt, dass es sich auch in der Praxis um Behörden handelt, die organisatorisch nichts miteinander zu tun haben.

B. Personelle Trennung

Bezüglich der personellen Trennung ist auf zwei Umstände hinzuweisen. Erstens ist der Innenminister zu erwähnen, der Weisungsrecht einerseits gegenüber der Polizei, andererseits gegenüber den drei Nachrichtendiensten, nämlich dem Verfassungsschutz, dem Fachdienst und dem Anti-Terror-Informations-und-Analysezentrum (TIBEK) hat. Die Person des Innenministers, der Teil der jeweiligen Regierung ist, verbindet demzufolge die Polizei – als Behörde der Strafverfolgung – mit den oben genannten Nachrichtendiensten. Diese Regelung kann damit begründet werden, dass dem Innenminister auf beiden Gebieten Aufgaben und Befugnisse eingeräumt sind, deshalb muss er imstande sein, sowohl die Strafverfolgung als auch die Nachrichtendienste betreffende Entscheidungen zu fassen und zu handeln.

Zweitens muss auf § 20 Abs. (1a) Nbtv. hingewiesen werden, wonach der TIBEK als Dienststelle der kooperierenden Organe, zu denen auch die Polizei und das Nationale Steuer- und Zollamt gehören, bestimmt werden kann. Diese gesetzliche Vorschrift ermöglicht also einen personellen Zusammenschluss der Strafverfolgungsbehörden und der Nachrichtendienste. Dies kann zur Folge haben, dass jemand, der früher bei der Ermittlungsbehörde beschäftigt war, später bei einem Nachrichtendienst tätig wird. Allerdings bezieht sich diese Vorschrift nur auf das Anti-Terror-Informations-und-Analysezentrum (TIBEK), bei den übrigen Nachrichtendiensten kann ein solcher personeller Austausch nicht stattfinden.

C. Funktionale Trennung

Die funktionale Trennung folgt grundsätzlich der organisatorischen Trennung oder umgekehrt, was heißt, dass die Strafverfolgungsbehörden ihre gesetzlich bestimmten Aufgaben entsprechend den Vorschriften der uStPO und den eigenen Rechtstellungsgesetzen erfüllen, während die Nachrichtendienste bei ihren Verfahren auf die Bestimmungen des Nbtv. Rücksicht zu nehmen haben. Die Trennung aufgrund der Funktionen der Strafverfolgungsbehörden und der Nachrichtendienste ist aber nur auf den ersten Blick eindeutig, denn sobald man die Tätigkeiten der Behörden unterschiedlicher Art näher betrachtet, muss festgestellt werden, dass die Grenzen nicht so deutlich gezogen sind.

Die grundlegende gesetzliche Bestimmung diesbezüglich ist § 31 Abs. 1 Nbtv., wonach den Nachrichtendiensten keinerlei ermittlungsbehördliche Befugnisse eingeräumt sind. Die uStPO enthält ihrerseits keine entsprechende Ausschluss-Klausel. Sie benennt lediglich abschließend die Behörden, die befugt sind, im Strafverfahren zu handeln. Keiner von den Nachrichtendiensten wird hierbei erwähnt. Hervorzuheben ist es allerdings an dieser Stelle § 36 Abs. 1 uStPO. Hiernach wird ein Vorbereitungsverfahren durchgeführt, in dem nicht nur die Ermittlungsbehörde und die Staatsanwaltschaft, sondern auch andere Behörden tätig werden dürfen, die befugt sind, auf verdeckte Ermittlungsmaßnahmen zurückzugreifen. Hierzu gehört auch die Terror-Abwehr-Einheit der Polizei (TEK). Außerdem ermächtigt § 244 uStPO die Strafverfolgungsbehörden, die Nachrichtendienste um Amtshilfe bei der Durchführung verdeckter Ermittlungsmethoden im Strafverfahren zu ersuchen, wenn sie diese nicht selbst anwenden können.

In Anbetracht des Gesagten lässt sich feststellen, dass die Strafverfolgung sowohl das reguläre Strafverfahren als auch die geheime Aufklärung davor umfasst. Zu Letzterer wird unter anderem die Tätigkeit der Nachrichtendienste und die der Terror-Abwehr-Organe gezählt. Diese geheime Aufklärung wird „Aufklärung außerhalb des Strafverfahrens“ genannt, und sie kann auch von polizeilichen Organen, die nicht Ermittlungsbehörden sind, betrieben werden. Sie ist dadurch gekennzeichnet, dass die gesetzlichen Bestimmungen hierfür lockerer sind als im Strafverfahren, weil eine viel zu ausführliche Regelung der Effektivität im Wege stünde. Die Gegenstände dieses Verfahrens sind Geschehnisse der Vergangenheit, der Gegenwart oder auch der Zukunft, die für die nationale Sicherheit oder aus polizeilicher Sicht ein Risiko darstellen.[43]

Die Nachrichtendienste betreiben ihre Aufklärung also in einem viel breiteren Spektrum als die Strafverfolgungsbehörden. Wenn die Ergebnisse der nachrichtendienstlichen Aufklärung im Strafverfahren verwendet werden sollen, gelten die Vorschriften der uStPO.

---

[43] Finszter Géza/Korinek László: Az eltűnt gyanú nyomában *in*: Belügyi Szemle 2018/3.

D. Informationelle Trennung

Die Informationsbeschaffung ist nicht nur der modus operandi von Nachrichtendiensten, sondern liegt inzwischen auch im Zentrum der strafprozessualen Tätigkeit.[44] Je nachdem, zu welchem Zweck und von welcher Behörde die Beschaffung von Informationen erfolgt, variieren die Voraussetzungen für diese Tätigkeit. Mit Hinblick auf den jeweiligen Zweck wird zwischen kriminalitätsbezogener und nachrichtendienstlicher Informationsbeschaffung unterschieden. Nach Péter Nyeste unterscheiden sich die beiden voneinander nur in wenigen Zügen. Die nachrichtendienstliche Informationsbeschaffung („personen- und gruppenorientierte Aufklärung") geschieht auf Antrag der jeweiligen Regierung. Die Richtigkeit der Informationen muss hier nicht vor Gericht bestätigt werden, aber die Folgen einer Entscheidung, die aufgrund falscher Informationen getroffen wurde, betreffen das ganze Land Ungarn. Die andere Art der Informationsbeschaffung – nach dieser Unterscheidung – ist die kriminalitätsbezogene Informationsbeschaffung, die „deliktorientierte Aufklärung". Abstrakt formuliert verlangt hier das Gesetz, das vom Täter verletzt wurde, die Herbeischaffung von Informationen. Diese Tätigkeit soll letztendlich der Beschaffung von Beweisen dienen.[45]

Die Strafverfolgungsbehörden und die Nachrichtendienste sind gesetzlich ermächtigt, persönliche Daten, die zur Erfüllung ihrer gesetzlich bestimmten Aufgaben notwendig sind, zu sammeln. Die geheime Informationssammlung/Anwendung von verdeckten Ermittlungsmethoden ist eine besondere Art der Beschaffung von Informationen. Mit Ausnahme des Analysezentrums steht diese Befugnis den Nachrichtendiensten zu, und auch die Ermittlungsbehörden und die Staatsanwaltschaft sind befugt, „geheim zu ermitteln".

Nach § 214 uStPO erfolgt die Anwendung von verdeckten Ermittlungsmethoden zu Strafverfolgungszwecken immer den Vorschriften der uStPO entsprechend. Die geheime Informationssammlung zu Strafverfolgungszwecken, die von den Nachrichtendiensten oder vom Terror-Abwehr-Organ der Polizei (TEK) geführt wird, bleibt davon unberührt.[46] Daraus folgt erstens, dass zum selben Zweck unter verschiedenen Voraussetzungen geheim Informationen gesammelt werden können, denn je nachdem, welche Behörde handelt, wird das Verfahren entweder nach den Vorschriften der uStPO oder nach dem Nbtv. geführt. Die zweite Folge ist, dass im Interesse der Strafverfolgung bei der Beschaffung von Informationen auch nachrichtendienstliche Methoden angewendet werden können.

---

[44] Finszter Géza: Közrend – közbiztonság – jogbiztonság (2000–2015).

[45] Nyeste Péter: A bűnüldözési célú „titkos információszerzés" és a büntetőeljárás kapcsolata *in*: Nemzetbiztonsági Szemle MMXIII/I.

[46] § 214 Abs. 3 uStPO.

Interessant ist auch, was mit den erhobenen Informationen geschieht, an welche Behörde sie übermittelt werden können und in welchem Fall sie übermittelt werden müssen.

Nach § 111 uStPO besteht für die Ermittlungsbehörden, für die Staatsanwaltschaft und für die Gerichte eine Meldepflicht. Das heißt, wenn diese während des Strafverfahrens auf Informationen stoßen, die für eine andere Behörde von Relevanz sind, verständigen sie die zuständige Behörde. Umgekehrt sind die Strafverfolgungsbehörden befugt, für sie relevante Informationen durch Amtshilfe bei anderen Behörden zu beschaffen.[47] Die ersuchte Behörde ist verpflichtet, das Amtshilfeersuchen der Strafverfolgungsbehörden zu erfüllen, falls ein Gesetz nichts anderes vorschreibt[48]. Die Erfüllungspflicht betrifft grundsätzlich auch die Nachrichtendienste. Allerdings stellt § 44 Abs. 21 Nbtv die Nachrichtendienste von dieser Erfüllungspflicht frei, wenn eine Informationsübermittlung ihre gesetzlichen Aufgaben gefährden würde. Dies gilt auch für die Einleitung des Strafverfahrens.

Einer weiteren Vorschrift der uStPO zufolge können die Beweise und die Unterlagen des Verfahrens, die im Rahmen der Verwendung von verdeckten Ermittlungsmittel beschafft worden oder zu Stande gekommen sind, den Nachrichtendiensten noch vor dem Abschluss des verdeckten Verfahrens bekannt gemacht werden.[49]

Die Nachrichtendienste sind ermächtigt, u.a. bei den Strafverfolgungsbehörden um die Übermittlung von Daten zu ersuchen, genauso, wie sie von den nationalen und mehreren internationalen (VIS, SIS z.B.) Datenbanken Daten abrufen können, die zur Erfüllung ihrer gesetzlichen Aufgaben notwendig sind. Das Gesetz bestimmt detailliert die Voraussetzungen für diese Informationsbeschaffung, aber wenn die Voraussetzungen erfüllt sind, haben die Nachrichtendienste zu Daten aller Art – auch zu den Daten der Strafverfolgung – Zugang.

Die Ermittlungsbehörden und die Staatsanwaltschaft sind befugt, zu dem in ihrem eigenen Rechtstellungsgesetz bestimmten Zweck selbst geheim Informationen zu sammeln. Die Nachrichtendienste können die Informationen, die im Rahmen eines solchen Verfahrens erhoben wurden, ebenfalls erhalten, falls das zur Erfüllung ihrer gesetzlich bestimmten Aufgaben nötig ist.

Aus den Vorschriften, auf die ich mich bezogen habe, folgt, dass die nationale Sicherheit höchste Priorität genießt, denn zu diesem Zweck müssen die relevanten Daten für die zuständigen Behörden unbegrenzt zugänglich gemacht werden, während die Nachrichtendienste aus diesem Grund die Nachrichtenübermittlung an anderen Behörden – auch an Behörden der Strafverfolgung – verweigern können.

---

[47] § 261 Abs. 1 uStPO.

[48] § 264 Abs. 1 uStPO.

[49] § 250 Abs. 3 lit c) uStPO.

V. Fazit – Vernachrichtendienstlichung der Strafverfolgung?

Manche Vorschriften der neuen uStPO stießen schon vor dem Inkrafttreten des Gesetzes auf heftige Kritik. Hierzu gehören insbesondere die Vorschriften, die unabhängig von einem Anfangsverdacht den Weg zur Anwendung von „geheimdienstlichen" Methoden öffnen.

Ágnes Czine (Verfassungsrichterin) beanstandet die Unklarheit der besagten Vorschriften bezüglich der Personen, gegen die die verdeckten Mittel angewendet werden können. Damit bezieht sie sich auf § 343 Abs. 1 lit. b) uStPO, in dem es heißt, dass sie „auch gegen die Personen, bei denen zu vermuten ist, dass sie mit der Person, die als Täter in Frage kommt, mittelbar oder unmittelbar Kontakt pflegen" angewendet werden können. Nach Ágnes Czine ist es zudem fraglich, ob diese Vorschrift mit der Rechtsprechung des EGMR in Einklang steht, konkret, ob sie den Verhältnismäßigkeitstest besteht. Denn die Anwendung von verdeckten Ermittlungsmaßnahmen beeinträchtigt die Privatsphäre des Einzelnen, und damit eine solche Beeinträchtigung der Menschenrechte gerechtfertigt ist, müssen gewisse Voraussetzungen erfüllt sein.[50]

Auch andere Autoren stimmten dieser Kritik zu. Weder die Notwendigkeit der Durchführung von besagten Ermittlungsmethoden im Strafverfahren noch deren Verhältnismäßigkeit könne ohne Anfangsverdacht begründet werden. Denn ohne das Vorliegen eines Anfangsverdachts könne überhaupt nicht bestimmt werden, ob für die Strafverfolgung relevante Informationen fehlen und welche diese sind. Außerdem stellt sich die Frage, wo dann die Grenze der polizeilichen Aufklärung liegt, unter welchen Voraussetzungen die geheime Informationssammlung außerhalb des Strafverfahrens stattfinden kann, wenn ein Anfangsverdacht nicht einmal im Strafverfahren erforderlich ist.[51]

Géza Finszter meint, dass das Erscheinen von neuen Formen der Kriminalität in der Tat neue Lösungen seitens der Strafverfolgung erfordert, aber die neuen Lösungen dürften niemals zur Folge haben, dass die Prinzipien der Rechtsstaatlichkeit aufgegeben werden. Das würde zur Willkür der Staatsgewalt führen.[52]

Das ungarische Verfassungsgericht hat das Interesse an der Kriminalprävention als verfassungsmäßigen Zweck anerkannt, der aus der Rechtsstaatlichkeit folgt und in dessen Interesse bestimmte Grundrechte beschränkt werden können. In allen einschlägigen Entscheidungen wurde aber betont, dass zu diesem abstrakten Zweck keines der Staatsorgane zu breite Befugnissen oder Ermächtigungen mit unklarem Inhalt erhalten soll.[53]

---

[50] Czine Ágnes: Gondolatok az új büntetőeljárási törvény kapcsán avagy leplezett eszközökkel leplezetlenül?

[51] Finszter Géza/Korinek László: Az eltűnt gyanú nyomában *in*: Belügyi Szemle 2018/3.

[52] Finszter Géza: Közrend – közbiztonság – jogbiztonság (2000–2015).

[53] Finszter Géza: Közrend – közbiztonság – jogbiztonság (2000–2015).

Die Kriminalprävention im Allgemeinen wurde mit der neuen Vorbereitungsphase zu einem selbständigen Zweck der Strafverfolgung erklärt. Der Begründung des Nbtv. zufolge wirken auch die Nachrichtendienste an der Strafverfolgung mit, weil die Straftaten gleichzeitig politische und nationale Sicherheitsinteressen des Staates gefährden können. Die ungarische Antwort auf neue globale Herausforderungen im Bereich Strafverfolgung ist also die uStPO mit ihren Neuerungen, die mehr Raum für die nachrichtendienstlichen Methoden im Rahmen des Strafverfahrens schaffen und die Schwelle zum Tätigwerden der Strafverfolgungsbehörden deutlich herabgesetzt haben.

Literaturverzeichnis

Finszter Géza: Közrend – közbiztonság – jogbiztonság (2000–2015) *in*: Biztonsági kihívások a 21. században.

Finszter Géza/Korinek László: Az eltűnt gyanú nyomában *in*: Belügyi Szemle 2018/3.

Nyeste Péter: A titkos információgyűjtés és a leplezett eszközök, a felderítés új modellje *in*: Belügyi Szemle, 2018/5.

Nyeste Péter: A bűnüldözési célú „titkos információszerzés“ és a büntetőeljárás kapcsolata *in:* Nemzetbiztonsági Szemle MMXIII/I.

Vida Csaba: A nemzetbiztonsági tevékenység szerepe a társadalomban.

Czine Ágnes: Gondolatok az új büntetőeljárási törvény kapcsán avagy leplezett eszközökkel leplezetlenül?

Mészáros Bence: A bűnügyi hírszerzés új rendszere hazánkban.

Abkürzungsverzeichnis

uGG	das Grundgesetz von Ungarn, von 25. April 2011 (ohne Nummer)
uStPO	Gesetz Nr. XC aus dem Jahre 2017 über das Strafverfahren
Nbtv.	Gesetz Nr. CXXV aus dem Jahre 1995 über die nationalen Sicherheitsdiensten
Ütv.	Gesetz Nr. CLXIII aus dem Jahre 2011 über die Staatsanwaltschaft
Rtv.	Gesetz Nr. XXXIV aus dem Jahre 1994 über die Polizei
NAV tv.	Gesetz Nr. CXXII aus dem Jahre 2010 über das Nationale Steuer- und Zollamt

Vergleich

Marc Engelhart und Mehmet Arslan

Die Nachrichtendienste sind in bestimmten Bereichen der schweren Kriminalität in letzter Zeit deutlich aktiver geworden, so dass Kriminalitätsbekämpfung zunehmend eine Angelegenheit der nationalen Sicherheit wird. Diese Entwicklung war in allen untersuchten Ländern zu verzeichnen. In einigen Ländern, wie den Niederlanden, Griechenland, Spanien und der Türkei hat die polizeiliche Prävention schon immer die Informationssammlung über Kriminalität umfasst. Man kann insofern von einer traditionellen nachrichtendienstlichen Funktion der Polizei sprechen. Auch in einem Bundesstaat wie der Schweiz ist dieses Phänomen auf Kantonsebene seit langem bekannt.[1] Neu scheint insbesondere der Umstand zu sein, dass nun auch die Hauptnachrichtendienste der Länder zum Einsatz kommen. Auffällig ist dabei, dass man den Aufbau von Massenüberwachungsmaßnahmen unter anderem mit der Verhinderung schwerer Kriminalität begründet. Die Dienste sollen

[1] Zur umstrittenen Geltung des Trennungsgebots auf der Landesebene in Deutschland siehe *Zöller*, Informationssysteme und Vorfeldmaßnahmen, S. 318; *Engerhart*/*Arslan*, Security Architecture, S. 59; vgl. *Poscher*/*Rusteberg*, Die Aufgabe des Verfassungsschutzes. Zur funktionalen Trennung von Polizei und Nachrichtendiensten, Kritische Justiz 2014/1, S. 58 vd.

nicht nur in der Sache helfen, sondern man will offenkundig das durch schwere Gewaltakte, sei es im eigenen Land (etwa in Spanien 2004 und Belgien 2016) oder auch nur über Bilder (etwa 9/11 in den USA) aus dem Ausland vermittelte, scheinbar erheblich geschädigte Sicherheitsgefühl im Alltag wiederherstellen.[2] Beispielhaft kann hierbei die 2017 verabschiedete neue Gesetzgebung in der Schweiz genannt werden, die die Befugnisse des schweizerischen Nachrichtendienstes des Bundes deutlich ausweitete und mit einer Mehrheit von 65,5 % der abgegebenen Stimmen angenommen wurde.

Dass die Dienste – wie an verschiedenen Indikatoren ablesbar ist – auch Akteure der Verbrechensbekämpfung sind, wird in den untersuchten Ländern kaum im Zusammenhang mit der gesamten Sicherheitsarchitektur betrachtet und analysiert, obwohl zumindest die sicherheitsbehördlichen Strukturen in den Ländern auf eine gewisse Architektonik hinweisen. Hinzu kommt, dass normative Bewertungsmaßstäbe fehlen, die sich in ein mehr oder weniger ausgearbeitetes Konzept einfügen lassen würden. Dadurch lässt sich die Entwicklung, die zu einer Zunahme der zwischen den Nachrichtendiensten und den Verbrechensbekämpfungsorganen bestehenden Berührungspunkte führt, kaum umfassend und systematisch einer normativen Würdigung unterziehen, obwohl diese in allen Ländern, wie die Autoren berichten, auch mit Argwohn verfolgt wird. Mit den neuen Befugnissen erlangen die Dienste Massendaten, und diese sind auch für die Strafverfolgung von großer Bedeutung. Die neu geschaffenen Interaktionswege informationeller Natur lassen spätestens im Strafverfahren beachtliche Probleme entstehen, deren Lösung die Strafgerichte vor neue Herausforderungen stellt.

Diese Befunde hinsichtlich der Strukturfrage (I.), der Berührungspunkte (II.) und der Interaktionswege (III.) werden im Folgenden veranschaulicht.

I. Strukturfrage

In allen hier betrachteten Ländern wird zwischen Prävention und Repression zumindest funktional unterschieden. Allerdings wird insbesondere die Prävention auf der polizeilichen Ebene weit und vage gefasst. Unterscheidungen wie konkrete und abstrakte Gefahr sind innerhalb des Polizeirechts kaum anzutreffen. Insofern fehlt ein klar herausgearbeitetes Recht der Gefahrenabwehr in Ländern wie Bulgarien, Griechenland, Rumänien, Spanien, Ungarn und der Türkei. Dies führt nicht zuletzt dazu, dass die polizeiliche Prävention vor allem als Verbrechensbekämpfung durch Informationssammlung verstanden wird und dadurch die Abteilungen polizeilicher Nachrichtendienste (etwa in Griechenland, Spanien, Ungarn und der

[2] Zur Problematik des subjektiven Empfindens der Sicherheit siehe *Albrecht*, Neue Bedrohungen?, S. 118 vd.; *Sieber*, Der Paradigmenwechsel, S. 353.

Türkei) ihre Berechtigung im System finden. Darunter leidet – soweit ersichtlich – der Schutz individueller Rechtsgüter durch ein klar abgegrenztes Gefahrenabwehrrecht. Hinzu kommt, dass die Strafverfolgung selbst zum Teil „Zulieferer der Prävention" geworden ist, jedenfalls in bestimmten Bereichen der Kriminalität wie dem Terrorismus und der organisierten Kriminalität. Die „strafprozessualen" Vorfeldermittlungen in der Schweiz und Ungarn, die ohne das Vorliegen eines irgendwie identifizierbaren Verdachts vonstattengehen dürfen, zeigen eine Entwicklung auf, die „Strafverfolgung" jenseits von materiellrechtlichen Erwägungen nicht als repressiv auffasst. So versteht das schweizerische Modell „Strafverfolgung" zumindest im Bereich des Extremismus und des Terrorismus als Teil eines holistischen Sicherheitszirkels. In Ungarn trägt das neue Vorfeldermittlungsverfahren deutliche Züge nachrichtendienstlicher Ermittlungen, wenn das neue Verfahren insbesondere auf die Ermittlungen im Umfeld von „Kontaktpersonen" abzielt.

Begriffliche Unklarheiten und ein stetiger Wandel der Inhalte scheinen ein Wesensmerkmal des Sicherheitsrechts zu sein. In einigen der untersuchten Länder, wie in Griechenland und den Niederlanden, wird auch angesichts der neuen Rolle der Nachrichtendienste in der Verbrechensbekämpfung ausdrücklich hinterfragt, was unter nationaler Sicherheit, deren Schutz in den ureigenen Aufgabenbereich der Nachrichtendienste fällt, zu verstehen ist. Während man in Griechenland diesen Begriff normativ zu erfassen und zu begrenzen versucht, so fällt in den Niederlanden die besondere Dynamik auf, die der Begriff etwa im Zusammenhang mit der Organisierten Kriminalität erfahren hat. Organisierte Kriminalität wurde in den Niederlanden ab 1992 als eine Bedrohung für die nationale Sicherheit betrachtet und seit 2000 dann wieder nicht mehr. In manchen Ländern, wie Griechenland, Ungarn, Spanien und Rumänien, wurde Organisierte Kriminalität, sobald sie einmal in den Beobachtungskatalog der Nachrichtendienste aufgenommen war, fortan als dauerhafte Bedrohung der nationalen Sicherheit angesehen. In Bulgarien kehrte die Polizeihauptdirektion zur Bekämpfung der organisierten Kriminalität zwischen 2013 und 2015 nach einem kurzen Aufenthalt bei der Staatlichen Agentur für die nationale Sicherheit (SANS) ins Innenministerium zurück.

Neben begrifflichen Unklarheiten, die die Bildung einer nationalen Sicherheitsarchitektur erschweren, bestehen auch offene Sachfragen, die allerdings teilweise kaum thematisiert werden. Das türkische Inlandsnachrichtendienstrecht ist in einem Gesetz aus dem Jahr 1934 geregelt und die darin verwendete Regelungstechnik ist alles anders als zeitgemäß. Wesentliche Begriffe eines Inlandsdienstrechts fehlen. Vor allem fehlt eine gesetzliche Bestimmung, was Gegenstand der Informationssammlung des polizeilichen Nachrichtendienstes (EIDB) ist. Ob der Dienst etwa über bestimmte politische Bestrebungen gegen die Rechtsgüter der inneren Sicherheit oder auch darüber hinausgehend zu allen Arten der Kriminalität Informationen sammeln soll, lässt sich aus dem Gesetz nicht entnehmen. Auch der Zweck der Informationssammlung lässt sich gesetzlich nicht klar ableiten. Eine ausdrückliche

Beschränkung auf die Beratung von politischen Entscheidungsträgern ist nicht ersichtlich.

Von einem „komplexen und unübersichtlichen Regelwerk“ des nationalen Nachrichtendienstes (EYP), das etwa kaum Eingriffs- und Ermittlungsschwellen enthält, berichtet auch *Ntamadaki* für Griechenland.

Zusammenfassend lässt sich konstatieren, dass grundlegende Voraussetzungen zur Bildung einer funktionalen Sicherheitsarchitektur, z.B. eine klare Abgrenzung solch wesentlicher Begriffe wie „Prävention“ und „Repression“ und eine ausdrückliche Adressierung wesentlicher Aspekte eines Sicherheitsrechts, in mehreren der untersuchten Länder fehlen. Die Behebung dieser Probleme bedarf einer ernsthaften juristischen Anstrengung.

II. Nachrichtendienste – Neue Ermittlungsorgane?

Die Nachrichtendienste beschränken sich nicht mehr auf die Beratung politischer Entscheidungsträger, sondern werden immer mehr zur Unterstützung exekutiver und auch judikativer Entscheidungen herangezogen. Dies lässt sich anhand neuer organisatorischer Strukturen und neu geschaffener Befugnisse wie folgt veranschaulichen.

A. Neu geschaffene Einheiten und Datenbanken

In einigen Ländern wurden im Bereich der Bekämpfung des Terrorismus und der Organisierten Kriminalität neue Einheiten und Datenbanken geschaffen. In Spanien bemüht man sich seit 2004, die Verbrechensbekämpfung in diesen Bereichen durch eine nachrichtendienstliche Informationssammlung zu unterstützen. 2014 vereinigte man bestehende Zentren unter dem CITCO (Intelligence Center against Terrorism and Organized Crime). Das Zentrum verfügt über zwei Datenbanken, nämlich das „Coordination of counter-terrorism Operations System“ (SICOA) und das „Investigations Coordination System“ (SCI). *Sánchez Ferro* berichtet, dass aus beiden Datenbanken Daten an die Polizei, Gerichte und Staatsanwaltschaften übermittelt werden können.

In Ungarn wurde 2016 das Anti-Terror Informations- und Analysezentrum (TIBEK) gegründet. *Margit Szabóné* weist darauf hin, dass das Zentrum wie eine Datenbank funktioniert. Es ist kein unmittelbares Strafverfolgungsorgan, sondern es sammelt unter anderem nachrichtendienstliche Informationen und versucht, „strafverfolgungsrelevante Verdachtsmomente abzuschöpfen“. Im Fall eines Verdachtes erfolgt dann eine Strafanzeige.

In den Niederlanden findet die Kommunikation zwischen dem nationalen Nachrichtendienst (AIVD) und den Strafverfolgungsorganen über das Counterterrorism Coordination Meeting (Algemeen Overlag Terrorismebestrijding) statt, wobei der AIVD auch eine sog. Counter Terrorist Infobox zur Verfügung stellt. Die Datenbank enthält Informationen über „Hochrisiko-Terroristen".

In Belgien interagieren die Nachrichtendienste und die Strafverfolgungsorgane über zwei Wege: das Coordination Organ for Threat Analysis (OCAD) und das Joint meetings of Standing Committees I and P. Soweit ersichtlich findet dabei kein Informationsaustausch in Bezug auf Einzelfälle statt. Die Übermittlung nachrichtendienstlicher Informationen an die Strafverfolgungsbehörden erfolgt über die sog. BIM-Kommission. Damit ist Belgien unter den untersuchten Ländern wohl das einzige, das die genannte Übermittlung einer institutionellen Garantie unterstellt.

In Griechenland existiert kein zentraler Koordinationsmechanismus zwischen dem nationalen Nachrichtendienst (EYP) und den Strafverfolgungsorganen. Jede Behörde hat ihre eigene Koordinationsstelle.

In der Türkei besteht ein gesetzlich vorgesehener Koordinationsmechanismus. Nähere Angaben darüber, ob und inwieweit er benutzt wird, sind jedoch nicht vorhanden.

Als neu geschaffene Behörden rücken schließlich die FIUs ins Blickfeld. In Griechenland und der Türkei scheinen diese Behörden einen gewissen Platz innerhalb der Sicherheitsarchitektur eingenommen zu haben, wobei sich die türkische FIU zunehmend als ein Nachrichtendienst versteht.

B. Ausbau des Überwachungsarsenals

Die Ausweitung der Überwachungsbefugnisse der Nachrichtendienste in den letzten Jahren lässt sich in einigen Ländern (Niederlande, Griechenland, der Schweiz und der Türkei) gut nachverfolgen. Im Jahr 2017 erhielt der niederländische AIVD nach dem Bericht von *Hijzen* neue Befugnisse. In Griechenland wurde 2008 der EYP mit neuen Befugnissen ausgestattet. In der Schweiz sind die Befugnisse des NDG wohl in einer nie dagewesenen Weise ausgeweitet worden. Augenfällig ist, dass der NDG nun auch befugt ist, personenbezogene Ermittlungen im Bereich des Terrorismus und Extremismus einzuleiten. Ein ähnlicher, konkreter auf Individualpersonen zugeschnittener Ansatz hat auch der AIVD in den Niederlanden.

In der Türkei sind die Befugnisse des MIT 2005 und 2014 ebenfalls deutlich ausgebaut worden.

III. Normative Grenzen der Interaktion zwischen den Nachrichtendiensten und der Strafverfolgung

In verschiedenen Ländern haben die Nachrichtendienste erst in den letzten Jahrzehnten eine parlamentarisch-gesetzliche Grundlage erhalten (Türkei 1983, Ungarn 1990, Bulgarien 1993, Spanien 2002). Bereits dieser Umstand zeigt, dass die normative Einhegung nachrichtendienstlicher Tätigkeiten durchweg auf eine junge Vergangenheit zurückblickt.

A. Grundprinzipien einer Sicherheitsarchitektur

In Deutschland ist das Trennungsgebot als Regulativ und Korrektiv hinsichtlich der Sicherheitsarchitektur von entscheidender Bedeutung.[3] Dieses Gebot ist z.B. in den Niederlanden, in Belgien und der Schweiz begrifflich bekannt, wobei seine Geltung und sein Umfang variieren. In den Niederlanden bekennt man sich am deutlichsten zum Trennungsgebot. In Belgien gerät es zunehmend unter Druck, wie *de Busser* berichtet. In der Schweiz dagegen scheint es nur in der Literatur eine gewisse Überzeugungskraft zu entfalten. In Bulgarien, Griechenland, Rumänien, Spanien, Ungarn und der Türkei fehlt ein auch normativ zu verstehendes Sicherheitskonzept.

In mehreren Ländern fanden in den letzten Jahrzehnten beachtliche Neustrukturierungen der Sicherheitsbehörden statt (Bulgarien, Griechenland, Spanien, Rumänien und Ungarn), und diese vermitteln nicht den Eindruck, einem gesamtheitlichen Sicherheitskonzept entsprungen zu sein, sondern sind wohl mehr unter den Eindrücken innenpolitischer Bedürfnisse entstanden (etwa in Bulgarien und Spanien). Eine schlüssige Sicherheitsarchitektur lässt sich dabei nur schwer formen, wenn Sicherheitsbehörden ständiges Experimentierfeld der Innenpolitik werden. Auch die immer wieder aufgetretenen Abhörskandale in einigen der untersuchten Länder (Bulgarien, Griechenland, Spanien) zeigen, wie die Nachrichtendienste für vermeintliche innenpolitische Gewinne instrumentalisiert werden können. Die ungarische Regelung, die dem auch die nachrichtendienstliche Überwachungsmaßnahmen umsetzenden Fachdienst untersagt, die Regierung über die gesammelten Informationen zu unterrichten, ist in diesem Zusammenhang eine besondere und strukturell interessante Vorkehrung.

Gleichzeitig ist nicht von der Hand zu weisen, dass die Dienste im Inland die Sicherheit unter anderem zu gewährleisten suchen, indem sie gerade die die verfassungsrechtliche Ordnung bedrohenden politischen Bestrebungen beobachten und dadurch zwangsläufig mit der Innenpolitik in Berührung kommen. Allerdings

---

[3] Hierzu siehe stellvertretend *Gusy*, Das verfassungsrechtliche Gebot der Trennung von Polizei und Nachrichtendiensten. ZRP 1987, 45–52.

gehen selbst derartig gut gemeinte Milieueinkesselungen auf Dauer zur Lasten der demokratischen politischen Vielfalt, wie man etwa in der Schweiz und den Niederlanden erst nach dem Wegfall des Eisernen Vorhangs bei der Beobachtung der sog. „subversiven" Bürger feststellte. In anderen Ländern (Bulgarien, Griechenland, Rumänien, Spanien und Ungarn) scheint die historische Erfahrung, dass die Dienste während des Kalten Krieges als reines Repressionsmittel fungierten, weiterhin lebendig zu sein. Dies führt zu einer fortbestehenden gewissen Skepsis gegenüber den Diensten; in Ländern wie Bulgarien und Rumänien sind gerade diese Dienste folglich am meisten in ihrer Reputation beeinträchtigt.

Auf dem Weg zu einem verfassungsrechtlich verankerten Trennungsgebot ist scheinbar Rumänien. Dessen Verfassungsgericht erachtete kürzlich ein Kooperationsprotokoll zwischen dem Inlandsdienst (SRI) und der Generalstaatsanwaltschaft für verfassungswidrig. Das Protokoll sah insbesondere vor, dass der SRI die von der Generalstaatsanwaltschaft ersuchten Überwachungsmaßnahmen ergriff und die Ergebnisse an diese übermittelte. Dadurch war die Strafprozessordnung klar umgangen. Das rumänische Verfassungsgericht unterstrich diesbezüglich, dass der SRI von Verfassungs wegen kein Gesetzesvollzugsorgan ist, durch ein Protokoll auch nicht zu einem solchen wird und die Generalstaatsanwaltschaft ihre Kompetenz nicht auf eine andere Behörde übertragen kann. Das genannte Protokoll verstoße gegen die Gewaltenteilung und die verfassungsrechtlich verankerte funktionale Aufteilung der sicherheitsbehördlichen Aufgabenfelder.

In einigen Ländern (Spanien, Bulgarien, Ungarn) spielt der Schutz von Grund- bzw. Menschenrechte eine gewisse regulative Rolle, zieht insbesondere den Ermittlungsbefugnissen einzelner Sicherheitsbehörden Grenzen und ebnet durch den Verhältnismäßigkeitsgrundsatz den Weg zu einem abgestuften System von Ermittlungsschwellen. Als in den Niederlanden 2017 die Nachrichtendienste eine völlig neue Gesetzgebung erhielten, zielte diese unter anderem darauf ab, die Befugnisse der Dienste EMRK-robust zu gestalten. Die Verrechtlichung der Dienste und deren Befugnisse erfolgte, wie *Novikov* ausführt, auch in Bulgarien im Zuge des auch unionrechtlich erforderlichen Grund- bzw. Menschenrechtsschutzes.

Der Aspekt des Grund- bzw. Menschenrechtsschutzes ist allerdings nicht überall gleich ausgeprägt. So kennt die türkische Verfassung zwar ein Grundrecht auf den Schutz personenbezogener Daten (Art. 20 Abs. 3 tVerf.), allerdings ist unklar, ob und inwieweit dieses Grundrecht nachrichtendienstlicher Informationserhebung-, -verarbeitung, -speicherung und -übermittlung etwa an die Strafverfolgungsorgane Grenzen zieht.[4]

---

[4] Das türkische Verfassungsgericht hat kürzlich im Zusammenhang mit der Sicherheitsüberprüfung die Bedeutung des Grundrechts auf Datenschutz hervorhoben und der Übermittlung personenbezogener Daten an die die Sicherheitsüberprüfung durchführende Behörde Grenzen gezogen, hierzu siehe tVerfG. E. 2018/163 K. 2020/13, Entscheidung v. 19.2.2020, in R.G. v. 28.04.2020, Nr. 31112, Rn. 9 vd.

B. Polizeiliche Nachrichtendienste und fehlende Inlandsdienste

In allen der hier untersuchten Länder sind die nationalen Nachrichtendienste grundsätzlich informationssammelnd tätig und damit nicht beauftragt, kriminalpolizeiliche Aufgaben, etwa die Beweissicherung oder gar auch eine Anklageerhebung, zu übernehmen. Das gilt jedenfalls für die zentralen Nachrichtendienste dieser Länder. Eine wichtige Ausnahme bilden in diesem Zusammenhang die polizeilichen Nachrichtendienste bzw. entsprechenden Abteilungen der Polizeibehörden.

In den Niederlanden sammelt die Polizei proaktiv Informationen etwa über Organisierte Kriminalität. In der Türkei hat sowohl die Polizei als auch die Gendarmerie Abteilungen, die sich ausdrücklich mit der nachrichtendienstlichen Informationssammlung zum Zwecke der Verbrechensbekämpfung befassen. In Belgien lässt sich ebenfalls eine Vergeheimdienstlichung innerhalb der Polizei beobachten. Auch in Ungarn wird die polizeiliche Informationssammlung als ein Bestandteil der Polizeiarbeit erachtet. In Griechenland hat die Hellenische Polizei einen Informationsdienst (DIDAP). In der Schweiz erfolgt die proaktive Informationssammlung durch die Polizei nicht zum Zwecke der inneren oder äußeren Sicherheit, sondern zur Aufdeckung von Straftaten. In Spanien haben Policía und Guardia Civil nachrichtendienstliche Abteilungen.

Bereits die obigen Ausführungen zeigen, dass Justiz und Exekutive in einigen Ländern immer noch nicht strikt voneinander getrennt sind, sondern insbesondere in Gestalt der Polizei in enger Kooperation stehen. Dies lässt sich bei der Unterscheidung der Kriminalpolizei und Verwaltungspolizei in Griechenland und der Türkei gut ersehen. In der Schweiz ist auf Kantonalebene etwa in Basel-Stadt die Staatsschutzbehörde innerhalb der Staatsanwaltschaft angesiedelt.

Augenfällig ist, dass der nationale Nachrichtendienst in einigen Ländern (Griechenland, Belgien, Niederlande, Schweiz, Spanien und der Türkei) sowohl für das Inland als auch für das Ausland zuständig ist. In allen diesen Ländern ist der nationale Dienst deutlich erkennbar in mehrere wichtige Felder der Verbrechensbekämpfung involviert. In einigen Ländern fehlt eine Begrenzung sogar ganz, sodass sie in allen Kriminalitätsfelder mit den Strafverfolgungsorganen kooperieren können (Griechenland und Rumänien bis 2018). In der Schweiz ist der NDB sowohl für das Inland als auch für das Ausland zuständig. Die CNI in Spanien ist ebenfalls im Inland tätig und pflegt insbesondere im Bereich des Terrorismus und der Organisierten Kriminalität eine enge Beziehung mit der Polizei und auch der Strafverfolgung.

Es stellt sich die Frage, ob eine Spaltung in Ausland- und Inlandsdienst dazu führen würde, dass sich die Nachrichtendienste weniger mit der Strafverfolgung befassen würden. Dies liegt aus zwei Gründen nahe. Mit einem Inlandsdienst könnte man erstens gut auf die polizeiliche Nachrichtensammlung verzichten. Eine

dadurch entlastete Polizei würde sich verstärkt für die Gefahrenabwehr im Einzelfall einsetzen. Zweitens würde ein sich auf sein Fachgebiet spezialisierender Dienst nicht so viel Interesse für die Strafverfolgung im Einzelfall haben. Allerdings wäre es voreilig, eine solche Aufteilung als Erfolgsmodell zu postulieren. Denn die Praxis in einigen Ländern zeigt, dass die Vorzüge der Trennung nicht durchweg vorhanden sind.

In Ungarn existiert ein Amt für Verfassungsschutz, das als Inlanddienst getrennt organisiert ist. Dennoch sind Vernachrichtendienstlichungstendenzen sowohl in der Polizei als auch in der Strafverfolgung (durch das neu eingeführtes Vorfeldermittlungsverfahren) beobachtbar. In Bulgarien ist der Inlandsdienst (SANS) und der Auslandsdienst (Staatliche Agentur der Geheimdienste) ebenfalls getrennt, jedoch mit der Folge, dass die SANS als eine „hybride" Struktur gedacht ist, die nachrichtendienstliche, präventiv-operative und strafverfolgende Funktionen innehaben soll.

Aus den genannten Beispielen lässt sich ableiten, dass die Existenz eines Inlandsdienstes allein noch keine Garantie dafür ist, dass dieser von der Verbrechensbekämpfung Abstand hält. Der rumänische Inlandsdienst (SRI) ist ein weiteres gutes Beispiel dafür. *Rinceanu* berichtet, wie diese Behörde bis Frühling 2018 auf der Grundlage eines zwischen ihm und der Generalstaatsanwaltschaft 2009 unterzeichneten Kooperationsprotokolls die Strafverfolgungsbehörden nicht nur im Bereich schwerer Kriminalität wie Terrorismus und Organisierter Kriminalität, sondern auch bei Steuerdelikten mit Informationen versorgte.

Als „hybride" Sicherheitsbehörden sind auch die beispielsweise in Griechenland, Ungarn und der Türkei neuerlich aufgrund internationaler Verpflichtungen eingeführten FUIs gedacht.

C. Personeller Austausch und vollzugspolizeiliche Befugnisse der Dienste

Die Frage einer Trennung von Polizei bzw. Justiz und Nachrichtendiensten betrifft auch die personellen Besonderheiten der Behörden. In diesem Zusammenhang sind erneut die nachrichtendienstlichen Abteilungen der Polizei zu erwähnen. Als polizeilicher Nachrichtendienst hat etwa der DIDAP in Griechenland „in Ausnahmefällen vollzugspolizeiliche Befugnisse". Auch in der Türkei gehören die Beamten der EIDB und des JIB zur Polizei, die gleichzeitig mit der Strafverfolgung beauftragt ist.

Die zentralen Nachrichtendienste haben aber überwiegend keine vollzugspolizeilichen Befugnisse. In Belgien hat der Staatssicherheitsdienst (VSSE) grundsätzlich keine Zwangsanwendungsbefugnisse, darf Zwang nur zum eigenen Personenschutz anwenden. Das gleiche gilt für die CNI in Spanien und wohl auch für den MIT in der Türkei. Auch in den Niederlanden, in Ungarn und in Rumänien haben die

Dienste keine vollzugspolizeilichen Befugnisse. In der Schweiz und in Griechenland haben der NDB und der EYP zusätzliche Befugnisse: im Fall der Schweiz betrifft dies, „in Computersysteme und -netzwerke im Ausland" einzudringen, „um den Zugang zu Informationen zu stören, zu verhindern oder zu verlangsamen" und im Fall von Griechenland, die „aktive Abwehr gegen elektronische Angriffe" zu leisten. Die beiden Ländern weichen somit, jedenfalls gesetzlich, von den übrigen ab und lassen die aktive Abwehr in der virtuellen Welt zu.

In einigen Ländern (Griechenland und Spanien) findet ein durchaus umfangreich ausgebauter Personenaustausch zwischen dem nationalen Nachrichtendienst und den anderen Sicherheitsbehörden einschließlich der Strafverfolgung statt. Dies ist auch ein Indikator für die Anbindung der Strafverfolgung an die Dienste.

D. Übermittlungsrecht und Strafverfahren

Die Frage einer Trennung betrifft schließlich die Übermittlung nachrichtendienstlicher Informationen an die Strafverfolgung und die anschließende Verwendung im Strafverfahren in Einzelfällen. Bei den polizeilichen Nachrichtendiensten erübrigt sich in den meisten Ländern wohl die Frage, ob die Übermittlung geregelt werden soll, weil ja alles in einer und derselben Behörde stattfindet. Eine Trennung von Prävention und Repression findet hier nicht statt. Auch hinsichtlich der (etwa in Spanien, Ungarn und den Niederlanden) neu geschaffenen Datenbanken sowie der FIUs (Griechenland und Türkei) ist die Übermittlungsfrage bislang scheinbar gar nicht oder kaum relevant.

In manchen Ländern (Bulgarien, Griechenland, Spanien und der Türkei) existiert kein ausführliches Übermittlungsrecht. In Ungarn können Strafverfolgungsorgane über den Weg der Amtshilfe die Herausgabe nachrichtendienstlicher Informationen beantragen. In den Niederlanden, der Schweiz und Spanien gehen nachrichtendienstliche Informationen als Amtsberichte an die Strafverfolgung. In manchen Ländern genießen die Nachrichtendienste bei der Übermittlung von Informationen an die Strafverfolgung einen breiten Ermessenspielraum (Griechenland, Schweiz und der Türkei). Außerdem sollten informelle Kommunikationswege, auf die etwa *Zurkinden* mit Blick auf den schweizerischen Nachrichtendienst des Bundes hinweist, in diesem Zusammenhang nicht außer Acht gelassen werden. Insofern hat auch ein umfassendes Übermittlungsrecht wohl eine begrenzte Leistungskraft. Belgien unterscheidet sich in dieser Hinsicht von den anderen hier betrachteten Ländern. Die Übermittlung erfolgt nicht unmittelbar vom Staatssicherheitsdienst an die Strafverfolgung, sondern nur über eine sog. BIM-Kommission.

Sind die nachrichtendienstlichen Informationen einmal ins Strafverfahren eingeführt, so sehen die hier betrachteten Strafprozessordnungen keine ausführlichen Regelungen vor, ob und unter welchen Voraussetzungen diese Informationen im Ermittlungs- und Hauptverfahren verwendet werden dürfen. Zum Teil enthalten die

Strafprozessordnungen (Griechenland, Spanien) oder auch Spezialgesetze (Türkei) ausdrückliche Bestimmungen, dass die Nachrichtendienste zum Schutz staatlicher Interessen von der Pflicht, Beweismittel an ein Strafgericht herauszugeben oder Zeugenvernehmungen zu genehmigen (Spanien), freigestellt werden können.

In der Schweiz ist die wohl wichtigste Voraussetzung, dass eine vergleichbare Maßnahme auch von der Staatsanwaltschaft hätte angeordnet werden dürfen. Andernfalls vermag aber der nachrichtendienstlich an die Strafverfolgung übermittelte Amtsbericht nicht nur einen Anfangsverdacht zu begründen, sondern darf auch als Grundlage für die Anordnung weiterer Zwangsmaßnahmen gegen den Beschuldigten herangezogen werden. Im gerichtlichen Hauptverfahren stellen sich dann die üblichen Probleme bezüglich der Verteidigungsrechte, wenn die nachrichtendienstlichen Informationen durch Beweissurrogate eingeführt werden. Im Ergebnis vermisst *Zurkinden* „in der Schweizer Praxis die Sensibilität für die Notwendigkeit eines (auch informellen) Trennungsgebots".

Die Ausführungen von *Sánchez Ferro* zeigen, dass sich in der spanischen Rechtswissenschaft etwa *Lorena Bachmaier* für die Schaffung rechtlicher Grundlagen hinsichtlich des Informationsflusses von den Diensten an die Strafverfolgung insbesondere im Bereich des Terrorismus stark macht, weil der Informationsfluss derzeit ungeregelt erfolge und dies kaum Rechtssicherheit biete. Dabei dürfen auf der Grundlage der übermittelten Amtsberichte (denuncia) der CNI Zwangsmaßnahmen wie etwa Durchsuchungsbefehle angeordnet werden. Im Hauptverfahren sei dagegen die Offenlegungsfrage hinsichtlich der eigentlichen Quellen der Amtsberichte kaum von Bedeutung, wenn andere Beweise für eine Verurteilung ausreichen. In den übrigen Fällen kann die CNI zum Schutz staatlicher Geheimnisse die Herausgabe von Dokumenten und die Genehmigung von Zeugenvernehmungen verweigern. Zur Wahrung der Verteidigungsrechte etablierte der Oberster Gerichtshof des Landes die Rechtsprechung, dass die Entscheidung der Regierung, Beweismittel zum Schutz staatlicher Geheimnisse im Strafverfahren nicht herauszugeben, im Wege eines In-camera-Verfahrens der rechtlichen Überprüfung durch den Gerichtshof unterzogen werden kann.

In der Türkei gelten einige Verwendungsverbote für die nachrichtendienstlich durch Telekommunikationsüberwachung erlangten Informationen zu anderen Zwecken einschließlich der Strafverfolgung. Allerdings ist die Reichweite dieser Verbote unklar, weil sich die höchstrichterliche Rechtsprechung mit diesen Fragen im Wege einer Rechtsfortbildung kaum befasst, sondern nur vordergründig auf Basis der Aktenlage prüft, ob der Schuldspruch in der Sache zutrifft. Der türkische Kassationsgerichtshof hat in diesem Zusammenhang nur das Gebot entwickelt, dass das Urteil nicht ausschließlich auf nachrichtendienstlichen Informationen beruhen darf. Diese Rechtsprechung führt dazu, dass über Beweissurrogate nachrichtendienstliche Informationen weiterhin ins Strafverfahren eingeführt werden können. Aufgrund nachrichtendienstlicher Informationen können auch Ermittlungsverfahren eingeleitet und Zwangsmaßnahmen ergriffen werden. Zum Schutz der Vertei-

digungsrechte bleibt den Beschuldigten (nur) die individuelle Verfassungsbeschwerde übrig.

In den Niederlanden dürfen die nachrichtendienstlichen Amtsberichte im Ermittlungsverfahren bei der Anordnung von Zwangsmaßnahmen benutzt werden und auch später können im Hauptverfahren Beamte des AIVD als Zeugen bei Ergeifen entsprechender Schutzmaßnahmen angehört werden.

Nachrichtendienstliche Informationen finden wohl auch in Bulgarien uneingeschränkt ihren Eingang in die Strafverfolgung. Allerdings versucht das bulgarische Strafverfahrensrecht die Gefahr, dass die Strafprozessordnung dadurch umgangen wird, durch ein Beweiswürdigungsverbot aufzufangen. Danach darf das Strafurteil nicht ausschließlich auf heimlich ermittelte Beweismittel (darunter fallen auch nachrichtendienstlichen Informationen) gestützt werden.

Der Umgehungsgefahr tritt in den untersuchten Ländern am entschiedensten das rumänische Verfassungsgericht entgegen. Nach der Rechtsprechung des höchsten Gerichts des Landes ist die Verwertung nachrichtendienstlicher Informationen, die durch Telekommunikationsüberwachung oder andere technische Mittel erlangt worden sind, im Strafverfahren unzulässig. In der griechischen Rechtsprechung hingegen ist ein Verwendungsverbot nachrichtendienstlicher Informationen im Strafverfahren noch nicht entwickelt worden.

Literaturverzeichnis

Albrecht, H.-J., Neue Bedrohungen? Wandel von Sicherheit und Sicherheitserwartungen in: P. Zoche, S. Kaufmann und R. Haverkamp (Hrsg.), Zivile Sicherheit. Gesellschaftliche Dimensionen gegenwärtiger Sicherheitspolitiken. Bielefeld 2010, 111–127.

Engelhart, Marc/Arslan, Mehmet, Security Architecture in Germany. Freiburg 2019.

Poscher, Ralf/Rusteberg, Benjamin, Die Aufgabe des Verfassungsschutzes. Zur funktionalen Trennung von Polizei und Nachrichtendiensten, Kritische Justiz 2014/1, 57–71.

Sieber, Ulrich, Der Paradigmenwechsel vom Strafrecht zum Sicherheitsrecht in: Tiedemann/Sieber/Burchard/Brodowski (Hrsg.), Die Verfassung moderner Strafrechtspflege. Erinnerung an Joachim Vogel, Baden-Baden 2016, 349–372.

Zöller, Mark Alexander, Informationssysteme und Vorfeldmaßnahmen von Polizei, Staatsanwaltschaft und Nachrichtendiensten: zur Vernetzung von Strafverfolgung und Kriminalitätsverhütung im Zeitalter von multimedialer Kommunikation und Persönlichkeitsschutz. Heidelberg 2002.

Gusy, Christoph, Das verfassungsrechtliche Gebot der Trennung von Polizei und Nachrichtendiensten. ZRP 1987, 45–52.

Comparison

Marc Engelhart and Mehmet Arslan

The intelligence services have recently become much more active in some areas of serious crime, and the fight against crime is increasingly a matter of national security. This development can be traced in all the countries examined in this study. In some countries, such as the Netherlands, Greece, Spain and Turkey, police prevention has always included information gathering on crime. In this context, one can speak of a well-known intelligence function of the police. In a federal state like Switzerland, this phenomenon has long been known at the cantonal level.[5] The fact that the main intelligence services of the countries examined are now also being used seems to be a novel factor. It is noticeable that the introduction of mass surveillance measures is justified, among other things, by the prevention of serious crime. The services should not only help in this matter but should also restore the considerably undermined feeling of security in everyday life due to sensational acts of violence, be it in one's own country (for example, in Spain in 2004 and Belgium

[5] For the controversial application of the principle of separation at the state level in Germany, see *Zöller*, Informationssysteme und Vorfeldmaßnahmen, 318; *Engelhart/Arslan*, Security Architecture, 59; compare with *Poscher, Ralf/Rusteberg, Benjamin*, Die Aufgabe des Verfassungsschutzes. Zur funktionalen Trennung von Polizei und Nachrichtendiensten, Kritische Justiz 2014/1, 58 ff.

in 2016) or only in the media (for example, 9/11 in the USA).[6] It is a paradigm that the new legislation passed in Switzerland in 2017, which significantly expanded the powers of the Swiss federal intelligence service, was adopted with a majority of 65.5% of votes.

The fact that the intelligence services are actors in the fight against crime in the countries examined in this study can be clearly shown by pointing out further indicators. In the countries studied, this situation is rarely evaluated from the point of view of an overarching security framework, despite the fact the structures of the security authorities in the countries indicate a certain architecture. In addition, there is a lack of normative criteria that make up a more or less elaborated concept. As a result, the development that has led to an increase in connections between the intelligence services and criminal prosecution organs can hardly be subjected to a comprehensive and systematic normative assessment even though, as the authors report, the mentioned development is occasionally followed with suspicion in the countries examined. With their new powers, the services can acquire massive amounts of data which is also of great importance for criminal prosecution. The newly created channels of interaction of an informational nature can cause considerable problems to arise in criminal proceedings, the solution of which poses new challenges for the criminal courts in the countries examined.

These findings regarding the structural question (I.), points of contact (II.) and interaction channels (III.) are illustrated in detail below.

I. Question of structure

In all the countries examined, a distinction is made, at least functionally, between prevention and repression. However, prevention, in particular at the police level, is broad and vague. Differentiations such as concrete and abstract danger within police law can hardly be found. In this respect, there is no clearly defined law to avert danger in individual cases in countries such as Bulgaria, Greece, Romania, Spain, Hungary and Turkey. Not least because of this, police prevention is primarily understood as the fight against crime through the collection of information and thus the departments of police intelligence services (e.g., in Greece, Spain, Hungary and Turkey) find their justification in the system. The protection of individual legal interests through a clearly delimited law to avert danger in these countries probably suffers from this. In addition, the criminal prosecution itself has become a supplier of prevention in some of the countries

[6] For the problem with the so-called subjective feeling of security see *Albrecht*, Neue Bedrohungen?, 118 ff.; *Sieber*, Der Paradigmenwechsel, 353.

examined, at least in some areas of crime, such as terrorism and organized crime. The "criminal" preliminary investigations in Switzerland and Hungary, which are allowed to take place without the existence of any identifiable suspicious elements, points to a development which, apart from substantive criminal law, does not understand the criminal prosecution, at least not primarily, as repressive. In clear terms, the Swiss model understands criminal prosecution, at least in the area of extremism and terrorism, as part of a holistic security circle. In Hungary, the new pre-field investigation procedure has clear characteristics of intelligence investigations as the new procedure is aimed at "contact persons".

Conceptual ambiguities and changes in their content seem to be an essential feature of security law. In some of the countries examined, such as Greece and the Netherlands, the new role of the intelligence services in the fight against crime is being expressly debated to the extent of what national security means, the protection of which falls within the intelligence services' remit. While scholars in Greece try to define and limit this term in a normative manner, the dynamism in the Netherlands, which this term has brought in with regard to organized crime, is notable. Organized crime was seen as a threat to national security in the Netherlands from 1992 onwards, but since 2000 this has not been the case. It is also noteworthy in this context that organized crime in some other countries examined, such as Greece, Hungary, Spain and Romania, once included in the "observation catalog" of the intelligence services, continues to be viewed by legislators and the services as a threat to national security. In Bulgaria, the Police Directorate for Combating Organized Crime returned to the Ministry of Interior between 2013 and 2015 after a short stay at the State Agency for National Security (SANS).

In addition to conceptual ambiguities, which make the formation of a national security architecture more difficult, there are also open questions that are rarely raised in some of the countries examined. The Turkish domestic intelligence service law is regulated in a code from 1934 and the regulation technique used in it is anything but contemporary. Essential terms of a domestic service law are missing. Above all, this applies to the lack of a statutory provision as to what is the subject of the information collected by the police intelligence service (EIDB). Whether the service is supposed to collect information about certain political endeavors against the interests of internal security or about all types of crime cannot be inferred from the mentioned code. In addition, the purpose of collecting information cannot be clearly deduced by law. An explicit restriction to advising political decision-makers is not evident.

Ntamadaki also reports on a "complex and unclear set of rules" pertaining to the Greek national intelligence service (EYP), which hardly contains any intervention and investigation thresholds.

In summary, it can be stated that the basic prerequisites for the formation of a functional security architecture, such as clear delimitation of essential terms, for

example, prevention and repression, and the explicit addressing of essential aspects of a security law, are missing in some of the countries examined. Solving these problems requires an open, serious legal effort.

II. Intelligence services – New criminal prosecution bodies?

Intelligence services are no longer limited to advising political decision-makers but are increasingly being utilized to support executive and judicial decisions. This can be illustrated in the countries examined, with their use of new organizational structures and newly acquired powers.

A. Newly created units and databases

In some of the countries studied, new units and databases have been created in the field of combating terrorism and organized crime. In Spain, efforts have been made since 2004 to support the fight against crime in these areas through gathering information by intelligence services. In 2014, existing centers were merged under the CITCO (Intelligence Center against Terrorism and Organized Crime). The center has two databases, namely, the Coordination of Counter-Terrorism Operations' System (SICOA) and the Investigation Coordination System (SCI). *Sánchez Ferro* reports that information from the two databases can be transmitted to the police, courts and public prosecutors.

In 2016, the Anti-Terrorism Information and Analysis Center (TIBEK) was founded in Hungary. *Margit Szabóné* points out that the center works like a database. It is not an actual criminal prosecution organ but, among other things, collects intelligence information and tries to "skim off suspicious cases relevant to criminal prosecution". In the event of suspicion, a criminal complaint will then be filed.

In the Netherlands, consultation between the national intelligence service (AIVD) and criminal prosecution agencies takes place via the Counterterrorism Coordination Meeting (Algemeen Overlag Terrorismebestrijding) and the AIVD also provides a so-called Counter Terrorist Infobox. The database contains information on "high-risk terrorists".

In Belgium, the intelligence services and criminal prosecutıon agencies interact in two ways: through the Coordination Organ for Threat Analysis (OCAD) and the joint meetings of Standing Committees I and P. As far as can be seen, no information exchange regarding individual cases takes place. The transmission of intelligence information to criminal prosecution takes place via the so-called BIM commission. Among all the countries examined, Belgium is probably the only one that subjects the above-mentioned transmissions to an institutional guarantee.

In Greece there is no central coordination mechanism between the National Intelligence Service (EYP) and the criminal prosecution agencies. Each authority has its own coordination point.

There is a coordination mechanism in Turkey, foreseen by law; however, there is no information on whether and to what extent it is used.

Finally, the FIUs come into consideration as newly created authorities. In Greece and Turkey, these authorities seem to have taken a certain place within the security architecture, with the Turkish FIU increasingly seeing itself as an intelligence service.

B. Expansion of the surveillance arsenal

The expansion of surveillance powers for the intelligence services in recent years can be clearly traced in some of the countries examined (the Netherlands, Greece, Switzerland and Turkey). In 2017, the Dutch AIVD received new powers, as reported by *Hijzen*. In 2008, the EYP in Greece was given new powers. In Switzerland, the powers of the NDG have arguably been expanded in an unprecedented way. It is obvious that the NDG is now also authorized to initiate investigations focused on single individuals in the area of terrorism and extremism. The AIVD in the Netherlands also has a similar approach tailored to specific individuals.

In Turkey, the MIT's powers were also significantly expanded in 2005 and 2014.

III. Normative limits of interaction between intelligence services and criminal prosecution

In some of the countries examined, the intelligence services have received a parliamentary legal basis over the last few decades (Spain in 2002, Hungary in 1990, Bulgaria in 1993, and Turkey in 1983). This fact alone shows that the normative framework of intelligence activities can look back on a very recent past.

A. Basic principles of a security architecture

In Germany, the principle of separation serves as a regulative and corrective instrument with regard to the security architecture. This requirement is conceptually known in some of the countries examined, such as the Netherlands, Belgium and Switzerland, although its validity varies from country to country. The Netherlands is most clearly committed to the separation requirement. In Belgium it is coming under increasing pressure, as *de Busser* reports. In Switzerland, on the other hand, it only seems to hold a certain persuasive power in the literature. In Bulgaria, Greece, Romania, Spain, Hungary and Turkey there is no normative security concept.

In some of the countries examined, considerable restructuring of the security authorities has taken place over the last few decades (Bulgaria, Greece, Spain, Romania and Hungary). This does not give the impression of having followed an overall security concept but, rather, of being influenced by domestic needs (e.g., in Bulgaria and Spain). A security architecture can hardly be created if security authorities become a constant field of experimentation for domestic politics. The wiretapping scandals that recur again and again in some of the countries studied (Bulgaria, Greece and Spain) show how the intelligence services can be instrumentalized for domestic political gains. The Hungarian regulation that prohibits the service from informing the government about the information collected, and which also facilitates intelligence surveillance measures, is an interesting precaution in this context.

At the same time, it cannot be denied that the domestic services try to ensure security, among other things, by observing political endeavors that threaten constitutional order, and as a result inevitably come into contact with domestic politics. However, even such well-intentioned milieu encirclements might only function at the cost of democratic political diversity in the long run, as was seen in Switzerland and the Netherlands after the fall of the Iron Curtain, with regard to the observation of so-called "subversive" citizens. In other countries examined (Bulgaria, Greece, Romania, Spain and Hungary), historical experiences of how the services functioned purely as a means of repression during the Cold War seem to be still alive. This probably leads to a certain skepticism towards the services in some of the countries studied (such as Bulgaria and Romania) and they are likely the ones most affected by a damaged reputation.

The Romanian Constitutional Court is on the way to developing a constitutionally anchored principle of separation. The court recently held a cooperation protocol between the domestic service (SRI) and the general public prosecutor's office as being unconstitutional. In particular, the protocol stipulated that the SRI should carry out the surveillance measures requested by the public prosecutor's office and forward the results to them. This clearly circumvented the Code of Criminal Procedure. The Romanian Constitutional Court underscored, in this regard, that the SRI is not a law enforcement body by virtue of constitution, and that the general public prosecutor's office cannot transfer its competence to another authority. The said protocol violates the separation of powers and the constitutionally anchored functional division of the remits of security authorities.

In some of the countries examined (Spain, Bulgaria and Hungary) the protection of basic or human rights plays a certain regulatory role, draws limits in particular to the investigative powers of individual security authorities, and, through the principle of proportionality, paves the way for a graduated investigation threshold system. When the intelligence services in the Netherlands gained completely new legislation in 2017, one of the aims of this was to make the powers of the services ECHR-robust. Creating a new parliament law for the services and their powers also

took place in Bulgaria, as *Novikov* explains, during the course of implementing the protection of basic human rights required under Union law.

However, the protection of basic or human rights is not the same in all the countries examined. The Turkish constitution recognizes a fundamental right to the protection of personal data (Art. 20, Paragraph 3 of the Constitution), but it is unclear whether and to what extent this basic right puts limitations on the collection, processing, storage and transmission of information to the criminal prosecution agencies.[7]

B. Police intelligence services and lack of domestic services

In all the countries examined, the national intelligence services generally collect information and are, therefore, not charged with taking on criminal investigations, such as securing evidence or bringing charges. At least this applies to the main services of the states. The police intelligence services and corresponding departments of the police authorities are an important exception in this context.

In the Netherlands, for example, the police proactively collect information about organized crime. In Turkey, both the police and the Gendarmerie have departments that are specifically tasked with the collection of intelligence information for the purpose of combating crime. In Belgium, there is also "intelligencing" or securitization within the police. In Hungary, too, the collection of information by the police is considered a part of police work. In Greece, the Hellenic Police have an information service (DIDAP). In Switzerland, the proactive collection of information by the police is not carried out for the purpose of internal or external security but to uncover criminal offenses. In Spain, the Policía and the Guardia Civil have intelligence departments.

The above statements clearly show that in some of the countries examined the judiciary and the executive are still not strictly separated from one another, but rather are in close cooperation within the police force. This can be observed particularly when differentiating between the criminal and administrative police in Greece and Turkey. In Switzerland, the state security authority is located within the public prosecutor's office at the cantonal level in Basel-Stadt.

It is noticeable that in some of the countries examined (Greece, Belgium, the Netherlands, Switzerland, Spain and Turkey) the national intelligence service is responsible for both domestic and foreign intelligence. In all of these countries, the

---

[7] The Turkish Constitutional Court recently emphasized the importance of the fundamental right to data protection in connection with security checks and set limits on the transmission of personal data to the authority carrying out the security check; see Decision of February 19, 2020 (E. 2018/163 K. 2020/13), in R.G. of April 28, 2020, No. 31112, margin 9 ff.

national service is clearly involved in some important areas of the fight against crime. In some countries there is even no limit so that they can cooperate with the law enforcement agencies in all areas of crime (implemented in Greece and Romania in 2018). In Switzerland, the NDB is active both domestically and abroad. The CNI in Spain is also active domestically and has close relationships with the police and criminal prosecution, especially in the field of terrorism and organized crime.

The question arises as to whether a split between the foreign and domestic services would result in the intelligence services becoming less concerned with criminal prosecution. This might seem obvious for two reasons. With a domestic service one could do without the police intelligence gathering. A police force relieved of this would do more to avert danger in individual cases. Second, a domestic service specializing in its remit would not be so interested in prosecuting individual cases. However, it would be premature to postulate such a split as a model for success because its implementation in some countries tells another story.

In Hungary there is an Office for the Protection of the Constitution, which is organized separately as a domestic service. Nevertheless, "intelligencing" or securitization tendencies can be observed both in the police force and in criminal prosecution (due to the newly introduced pre-field investigation proceedings). In Bulgaria, the domestic service (SANS) and foreign service are also separated, but with the result that the SANS is designed as a "hybrid" structure that has intelligence, preventive-operational and criminal prosecution functions.

From the examples mentioned above it can be deduced that the existence of a separate domestic service is no guarantee that it will keep its distance from the fight against crime. The Romanian Domestic Service (SRI) is another good example of this. *Rinceanu* reports how this authority, on the basis of a cooperation protocol signed between him and the general prosecutor's office in 2009, provided information to criminal prosecution not only in the area of serious crime, such as terrorism and organized crime, but also in relation to tax evasion offenses up until the spring of 2018.

The FUIs recently introduced on the basis of international obligations are also designed as "hybrid" security authorities in some of the countries examined (e.g., in Greece, Hungary and Turkey).

C. Personal exchange and law enforcement powers of the services

The question of separation also affects the peculiarities of the security services' personnel. In this context, the police intelligence departments in some of the countries examined should be mentioned again. As a police intelligence service, the DIDAP in Greece has in "exceptional cases police powers". In Turkey, too, the

officers of the EIDB and JIB belong to the police force, which is also responsible for criminal prosecution.

The main intelligence services in the countries examined, however, for the most part do not have any police enforcement powers. In Belgium, the State Security Service (VSSE) does not have any compulsory enforcement powers and may only use compulsion for the protection of its own personnel. The same applies to the CNI in Spain and also to the MIT in Turkey. In the Netherlands, Hungary and Romania, too, officials do not have any police enforcement powers. In Switzerland and Greece, however, the NDB and EYP have the power to penetrate "into computer systems and networks abroad" in order "to disrupt, prevent or slow down access to information" in the first case and in the second to "actively defend against electronic attacks". The two countries thus deviate, at least legally, from the other countries examined and allow active defense in the virtual world.

In some of the countries examined (Greece and Spain) there is a well-developed exchange of persons between the national intelligence service and the other security authorities, including criminal prosecution. This is also an indicator of how close criminal prosecution is to the intelligence services.

D. Transmission of intelligence information and criminal proceedings

The question of separation also concerns the transmission of intelligence information to the criminal prosecution and its subsequent use in criminal proceedings in individual cases. In the case of the police intelligence services, there is probably no need to ask whether the transmission should be regulated, because everything takes place within the same authority. A separation between prevention and repression does not take place here. Also, with regard to the newly created databases in Spain, Hungary and the Netherlands, and the FIUs (Greece and Turkey), the question of transmission seems to be redundant.

In some of the countries examined (Bulgaria, Greece, Spain and Turkey) there are no detailed regulations on transmission. In Hungary, criminal prosecution agencies may request intelligence information under the scheme of "administrative assistance". In the Netherlands, Switzerland and Spain, intelligence information is sent to criminal prosecution agencies as official reports. In some of the countries studied, the intelligence services enjoy a wide margin of discretion when transmitting information to criminal prosecution (Greece, Switzerland and Turkey). In addition, informal communication channels, which *Zurkinden* refers to in relation to the Swiss federal intelligence service, should not be disregarded in this context. In this respect, comprehensive regulations on transmission also have a limited capacity. Belgium differs in this context from the other countries examined. The transfer

does not take place directly from the state security service to the criminal prosecution, but only via a so-called BIM commission.

Once the intelligence service information has been introduced into criminal proceedings, there are also insufficient provisions in the criminal procedure codes in the countries examined as to whether and under what conditions it may be used during the investigation stage and main trial. In some of the countries examined, the criminal procedure codes (Greece and Spain) or special laws (Turkey) contain explicit provisions that allow intelligence services to be exempted from the obligation to transmit evidence to a criminal court or to approve the examination of witnesses (Spain) in order to protect state secrets.

In Switzerland, the most important requirement is that a comparable measure should have been ordered by the public prosecutor. Otherwise, the official report sent by the intelligence service to the criminal prosecution may not only justify a so-called "initial suspicion" but may also be used as a basis for ordering further coercive measures against the accused. In the court trial, the usual problems with the rights of the defendant arise when the intelligence information is introduced by means of evidence surrogates. The result, according to *Zurkinden*, is that "in Swiss practice a sensitivity to the necessity of an (also informal) principle of separation" is missing.

From the report by *Sánchez Ferro* it can be seen that in Spain *Lorena Bachmaier* has appealed to create a legal basis for the flow of information from the services to criminal prosecution, especially in the area of terrorism, because such a flow of information already occurs in an unregulated way and this hardly offers legal certainty. In the current legal situation, compulsory measures such as search warrants may be ordered on the basis of official reports (denuncia) sent by the CNI. In the court trial, the question of disclosure regarding the actual sources of the official reports would be of little importance if other evidence is sufficient for a conviction. In other cases, in order to protect state secrets, the CNI may refuse to hand over documents and permit the examination of witnesses. As a remedy for the rights of the defense, the state's highest court of justice has developed the case law, where the decision of the government not to hand over evidence in order to protect state secrets in criminal proceedings can be subjected to legal review by the court through an in-camera procedure.

In Turkey, there are some exclusion rules on the use of intelligence obtained through telecommunications surveillance for other purposes, including criminal prosecution. However, the scope of these rules is unclear because the Turkish Court of Cassation has very little to do with corresponding questions during the course of its review but is primarily concerned with the issue of whether the verdict is correct in the matter. In this context, the Turkish Court of Cassion has only developed the prohibition that the judgment may not be based exclusively on intelligence information. This jurisprudence means that intelligence information can continue to be

introduced into criminal proceedings via evidence surrogates. Based on information from the intelligence service, preliminary proceedings may also be initiated and compulsory measures may be taken. As a remedy for possible disadvantages suffered by the defense, the accused is forced to bring their individual constitutional complaint to the Turkish Constitutional Court.

In the Netherlands, official intelligence reports may be used in the preliminary proceedings to initiate coercive measures, and officials of the AIVD may also be heard as witnesses under protective measures later in the court trial.

Intelligence information will probably find its way into criminal prosecution in Bulgaria without restriction. However, Bulgarian criminal procedure law tries to avert the risk of circumventing the criminal procedure code by stipulating an exclusionary rule on evidence. According to this, the criminal judgment may not be based solely on evidence that has been gathered secretly (including intelligence information).

The Romanian Constitutional Court is the most decisive in countering the risk of circumvention in the countries examined. According to the case law of the highest court in the country, the use of intelligence information that has been obtained through telecommunications surveillance or other technical means is not permitted in criminal proceedings. An exclusionary rule on the use of intelligence information in criminal proceedings, on the other hand, has not yet been developed in Greece in jurisprudence.

References

Albrecht, H.-J., Neue Bedrohungen? Wandel von Sicherheit und Sicherheitserwartungen in: P. Zoche, S. Kaufmann und R. Haverkamp (eds) Zivile Sicherheit. Gesellschaftliche Dimensionen gegenwärtiger Sicherheitspolitiken. Bielefeld 2010, 111–127.

Engelhart, Marc/Arslan, Mehmet, Security Architecture in Germany. Freiburg 2019.

Poscher, Ralf/Rusteberg, Benjamin, Die Aufgabe des Verfassungsschutzes. Zur funktionalen Trennung von Polizei und Nachrichtendiensten, Kritische Justiz 2014/1, 57–71.

Sieber, Ulrich, Der Paradigmenwechsel vom Strafrecht zum Sicherheitsrecht in: Tiedemann/Sieber/Burchard/Brodowski (eds), Die Verfassung moderner Strafrechtspflege. Erinnerung an Joachim Vogel, Baden-Baden 2016, 349–372.

Zöller, Mark Alexander, Informationssysteme und Vorfeldmaßnahmen von Polizei, Staatsanwaltschaft und Nachrichtendiensten : zur Vernetzung von Strafverfolgung und Kriminalitätsverhütung im Zeitalter von multimedialer Kommunikation und Persönlichkeitsschutz. Heidelberg 2002.

Gusy, Christoph, Das verfassungsrechtliche Gebot der Trennung von Polizei und Nachrichtendiensten. ZRP 1987, 45–52.

ArchiS
Architektur des Sicherheitsrechts

Verbrechensbekämpfung durch Nachrichtendienste ist in zahlreichen Bereichen der schweren Kriminalität, wie Terrorismus, Cybercrime, organisiertes Verbrechen oder Wirtschaftskriminalität, mittlerweile kein unbekanntes Phänomen mehr. Diese Entwicklung wirft die Frage auf, ob und wieweit sich die Vernachrichtendienstlichung der Verbrechensbekämpfung konzeptionell umrahmen und normativ begründen lässt.
Der vorliegende Sammelband geht diesen Grundfragen des Sicherheitsrechts in neun europäischen Rechtsordnungen nach und fasst diese in einer vergleichenden Bewertung, die auf zahlreiche Defizite der bestehenden Rechtslage hinweist, zusammen.

In many European countries, the participation of intelligence services in the fight against crime is no longer an unknown phenomenon; it has been on the rise in these countries in numerous areas of serious crime such as terrorism, cybercrime, organized crime, and white-collar crime. This development raises the question whether and to what extent the increasing role of intelligence in fighting crimes can be conceptually framed and normatively justified.
This volume explores these basic questions of security law in nine European countries and summarizes the findings in a comparative assessment that points to numerous deficits in the existing legal situation.

ArchiS – Architektur des Sicherheitsrechts
c/o Max-Planck-Institut zur Erforschung
von Kriminalität, Sicherheit und Recht
Günterstalstr. 73
79100 Freiburg i. Br.
Germany

Tel. +49 (761) 7081-0
Fax +49 (761) 7081-294
info@csl.mpg.de
https://csl.mpg.de