Bundeskriminalamt

HERBST-TAGUNG 2013
BKA AUTUMN CONFERENCE

Cybercrime –

Bedrohung, Intervention, Abwehr

BKA-Herbsttagung vom 12. – 13. November 2013

Begrüßungsrede

Jörg Ziercke

Präsident des Bundeskriminalamtes

– Es gilt das gesprochene Wort. –

Wegen der dynamischen phänomenologischen Entwicklung, aber auch wegen der katalysierenden Wirkung, die das Internet als Tatmittel auf die Veränderung der modi operandi vieler Deliktsformen des Strafgesetzbuches, auf den Schadensumfang, auf viktimologische Aspekte sowie auf die Anforderungen an eine effektive Verbrechensbekämpfung hat, ist dies sicherlich ein Thema von hoher Aktualität. Dies zeigen auch die vielen Veranstaltungen in diesem Jahr, die sich mit dem Thema 'Cybercrime' beschäftigt haben. Das belegen viele Sondersitzungen der Polizeien des Bundes und der Länder. Alle reden über eine effektive Verbrechensbekämpfung im digitalen Zeitalter.

Noch vor 10 Jahren wurde in Statistiken der prozentuale Anteil von „Haushalten mit Internetanschluss“ bzw. die „Ausstattung von Haushalten mit PC“ erhoben – heute im Zeitalter von Smartphone, von Tablet, von Wlan-Hotspots, von SmartGrid fast anachronistisch anmutende Erhebungskriterien!

Wir sprechen von flüchtiger Moderne, vom Zeitalter der digitalen Revolution. Dies bringt Umwälzungen, die mit der industriellen Revolution vor 200 Jahren verglichen werden, in allen Lebensbereichen mit sich. Wegen der ihr immanenten Überschreitung jeglicher Art tradierter Ordnungsmuster und der Veränderungsgeschwindigkeit gehen diese Umwälzungen mehr und mehr in eine Nachdenklichkeit über, ob wir bereits in der Lage sind, auf die uns gestellten Fragen hinreichende Antworten zu geben.

Digitale Technologien haben alle Lebensbereiche, Kommunikations- und Interaktionsformen durchdrungen. Sie bieten uns große Chancen und Möglichkeiten. Sie sind eine bedeutende Lebensader unserer Welt geworden, prägen mehr denn je alle Entwicklungen einer rasant fortschreitenden globalen Vernetzung. Ihr Potenzial scheint unerschöpflich.

Damit einher gehen aber auch spezifische Abhängigkeiten, Bedrohungen, Verletzbarkeiten und spezifische subjektive Unsicherheitsgefühle.

Das, was wir unter Cybercrime zusammenfassen, ist eine Bedrohung mit unvergleichbarer Dimension: Allein die direkten Kosten, die durch Cybercrime entstehen, sind größer als jene, die der Handel von Kokain, Heroin und Marihuana gemeinsam erzeugen.

Betrugsdelikte und Erpressungen, Eigentum- und Diebstahlsdelikte, illegaler Handel mit Drogen, Kinderpornographie oder Geldwäsche und auch Cybercrime im Bereich der politisch-motivierten

Kriminalität: Durch die über das Internet zur Verfügung gestellte digitale Infrastruktur eröffnen sich neuartige modi operandi mit enormen Schadensausmaßen und -potenzialen.

Die Infrastruktur des Internet führt dazu, dass nicht nur Ordnungskriterien wie Zeit und Raum an Bedeutung verlieren. Sie führt ebenso dazu, dass die auf solchen Kriterien basierenden Rechtsordnungen – denken Sie nur an die klassischen Begriffe des Straf- und Strafprozessrechtes wie örtliche Zuständigkeit oder Tatzeit – an funktionale und territoriale Grenzen stoßen, ohne dass alternative Steuerungsmedien und -ebenen erkennbar sind. Das Internet entgrenzt Kriminalität und ist ungebremst entwicklungsoffen.

Unsere BKA-internen Analysen, basierend auf dem Szenario-Projekt zum Thema „Always-on-Gesellschaft“, zeichnen folgende Entwicklungslinien:

1. Die Zahl der potentiellen Einfallstore für Kriminelle steigt weiter: Je mehr Geräte und Schnittstellen wir nutzen, je stärker wir uns digital vernetzen, desto mehr nimmt die Verwundbarkeit der Systeme zu.
2. Der virtuelle Handel, virtuelle Währungen und Cyber-Terrorismus bilden auch künftig Schwerpunkte krimineller Internet-Aktivitäten.
3. Schnellere Übertragungstechnologien erhöhen die Datentransfers. Die Folge sind immer größere Datenmengen. Die Anforderungen an die Recherche- und Analysefähigkeiten im Strafverfahren steigen an.
4. Ein gemeinsames Verständnis, abgestimmte Arbeitsteilung zwischen den Sicherheitsbehörden, wie auch zwischen Behörden und Wirtschaft und anderen Institutionen – auch weltweit – wird immer wichtiger.

Was bedeuten diese Entwicklungslinien für unsere Arbeit?

Um Cybercrime zu bekämpfen, müssen wir die Bedrohungslage differenziert beschreiben und analysieren, müssen intervenieren, Gefahren abwehren und Straftaten verfolgen!

Es geht darum, Antworten auf folgende Fragen zu finden:

Wie muss kriminalpolizeiliche Arbeit heute und in der nahen Zukunft aussehen?

Welche kriminaltechnischen und forensischen Möglichkeiten brauchen wir?

Wie müssen sich die Sicherheitsbehörden aufstellen?

Welche Kooperationsformen sind notwendig?

Reicht die bestehende Gesetzeslage aus?

Damit einher geht die Frage: Wie schaffen wir es, das notwendige Vertrauen der Menschen in unserem Land in die polizeiliche Arbeit gegen gewissenlose Cyberkriminelle zu gewinnen und nicht als Totalüberwacher, Datensammelwütige oder Datenprofilneurotiker denunziert zu werden?

Wie gelingt es, in einem solchen Begriffseinheitsbrei Konturen zu bestimmen, die eine sach- und zweckdienliche Auseinandersetzung um den einzuschlagenden Weg erst ermöglichen?

Wie schaffen wir es, den Bürgerinnen und Bürgern verstehbar zu erklären, dass bei der Verfolgung von schwerer Kriminalität im Internet derzeit eine Gerechtigkeitslücke entsteht, die wieder einmal nur die Cleveren und Verantwortungslosen bevorteilt, aber den rechtstreuen Bürger fassungslos zurücklässt? Die auf Dauer unser Wert- und Normensystem zerstört, ohne das auch eine digitale Gesellschaft nicht zusammenhält.

Mich beschäftigt in diesem Zusammenhang die Frage, ob unsere bisherige Politikberatung wirklich ausreicht? Bund und Länder verständigen sich derzeit auf eine dem globalen Wirkungsraum der Täter entsprechenden Erfassung von Auslandsstraftaten in der Polizeilichen Kriminalstatistik.

Gemeint sind Angriffe auf deutsche Internetuser, Private wie Unternehmen, insbesondere Botnet-Angriffe, bei denen hunderttausende von Rechnern in Deutschland kompromittiert und sabotiert oder als kriminelles Werkzeug benutzt werden. Klare Gesetzesverstöße, die aber heute in keiner Statistik erscheinen. Eine Geschädigtenstatistik soll zukünftig Auskunft geben, ob 1, 2 oder 3 Millionen Menschen oder mehr pro Jahr von Cybercrime in Deutschland betroffen sind. Vielleicht können solche Zahlen die Debatte versachlichen.

Polizei- und auch die Arbeit der Justiz ist „Informationsverarbeitung“. Wir müssen Informationen erheben, selektieren und bewerten. Verdachtsschöpfung, Beweiserhebung, Beweissicherung und Beweisführung folgen im Zeitalter der Cybercrime anderen Logiken, anderen Regeln und Prozessen.

Digitale Spuren und Beweise sind ortsungebunden, flüchtig, veränderbar, zum Teil anonymisiert und kryptiert. Bewährte kriminalistische Methoden und Instrumente stoßen angesichts dieser Charakteristiken an ihre Grenzen.

Zum Beispiel: Maßnahmen der Telekommunikationsüberwachung sind wesentlich für den Ermittlungserfolg in Bereichen schwerer und schwerster Kriminalität. Nach Expertenmeinung ist die Ermittlungsarbeit bei Organisierter Kriminalität zwischen 60 bis 70 Prozent von funktionierender Telekommunikationsüberwachung essentiell abhängig. Doch die zunehmende Verschlüsselung und Kryptierung der Telefonie über das Internet führen dazu, dass Telekommunikationsinhalte mittels klassischer TKÜ-Maßnahmen nicht mehr zu erschließen sind.

In Zusammenarbeit mit den Bundesländern hat das Bundeskriminalamt 167 herausragende Fälle der Schwerkriminalität ausgewertet, in denen Ermittlungsdefizite entstanden sind, weil die Überwachung oder Auswertung von Telekommunikation rechtlich oder technisch aufgrund von Verschlüsselung oder Kryptierung nicht möglich war. In über 70 Prozent dieser Fälle konnte sogar die Art des Kryptierungsdienstes technisch genau belegt werden. Viele schwere und schwerste Straftaten konnten aufgrund des bestehenden Informationsdefizits folglich nicht verhindert und nicht verfolgt werden.

Auch die alternative Nutzung klassischer Maßnahmen wie der Observation oder der Wohnraumüberwachung helfen uns häufig nicht, die notwendigen Daten zu erheben!

Wir brauchen daher andere geeignete Maßnahmen, damit unsere Ermittlungen nicht ins Leere laufen: Ich spreche von der Möglichkeit der Zuordnung von IP-Adressen zu real existierenden Personen – also Mindestspeicherfristen bei den Providern, von Quellen-TKÜ und Onlinedurchsuchung in Fällen schwerster Kriminalität und als ultima ratio mit besonderen Anforderungen an den Grundsatz der Verhältnismäßigkeit.

Wir sind uns der Grundrechtseingriffstiefe und daher der Sensibilität im Umgang mit diesen Instrumenten sehr bewusst. Das Bundesverfassungsgericht selbst hat den Weg für eine verfassungsgemäße Umsetzung aufgezeigt und die Behauptung, die Polizei würde unschuldige Bürger mit einem Generalverdacht überziehen, zurückgewiesen.

Um sicher zu sein, dass die eingesetzte Software für Quellen-TKÜ und Onlinedurchsuchung nicht mehr kann als sie darf, dass technische Vorgaben eingehalten werden, setzen wir darauf, diese Tools selbst zu entwickeln.

Prozesse und Abläufe werden protokolliert, der Kernbereichsschutz wird fortlaufend durch von der ermittlungsführenden Dienststelle unabhängige Einrichtungen überwacht und nicht nur der Bundesbeauftragte für Datenschutz und Informationsfreiheit kann unsere Vorgehensweise jederzeit kontrollieren. Für die Beweiswürdigung durch den Richter müssen wir unsere Vor-

gehensweise ohnehin dokumentieren und offenlegen. Diese Transparenz sichert die Rechtmäßigkeit der Maßnahmen und den Schutz der Grundrechte der Bürger und das Vertrauen in den Rechtsstaat.

Es wäre allerdings zu kurz gegriffen, sich bei der kriminalistischen Methodenentwicklung ausschließlich auf die Anpassung bzw. Generierung digitaler Ermittlungsinstrumente zu kaprizieren. Diese sind technisch aufwendig und auf Grund der dynamischen Innovationszyklen von geringer Halbwertszeit.

Eine effektive Strafverfolgung und Gefahrenabwehr bedarf selbstverständlich eines ganzheitlichen Ermittlungsansatzes, das heißt einer auf den jeweiligen Einzelfall bezogenen Kombination aus Ermittlungsansätzen der digitalen und der analogen Welt. Beispielsweise durch verdeckte Informationsgewinnung mittels Oberservationen, den verdeckten Einsatz von Polizeibeamten, durch den Cyber-VE oder die Cyber-VP – Instrumente, die unerlässlich sind angesichts der einfacheren Abschottung der Kommunikation und Interaktion von Tätern im Internet.

Zudem treiben wir den Aufbau einer kriminaltechnischen Servicestelle weiter voran. Das so genannte Cyberlab umfasst die Kryptoanalyse und Dekryptierung von Verschlüsselungen, die Softwareanalyse der Funktionen von digitalelektronischen Asservaten (inkl. „Apps“) und die Administration von Spezialrechnern sowie eines Labornetzes.

Aktuell befasst sich eine Projektgruppe der Polizeien des Bundes und der Länder mit dem Aufbau einer sicheren IT-Infrastruktur zur automatisierten Bearbeitung von Foto- und Videodaten.

Nach den Terroranschlägen in Boston im April dieses Jahres erhielten die US-amerikanischen Sicherheitsbehörden nach einem öffentlichen Fahndungsaufruf innerhalb weniger Stunden über eine Million Fotos und mehr als 1.000 Stunden Videomaterial unterschiedlichster Formate und Quellen. Zur Aufbereitung dieser Datenmengen für die Fahndung und Ermittlungen haben die US-Amerikaner eine Spezialeinheit eingerichtet, die aus über 50 geschulten Videoanalysten besteht und eng mit Universitäten und anderen Einrichtungen kooperiert.

Auch die Polizeien von Bund und Ländern müssen bei vergleichbaren Ereignissen – ich erinnere an die Tasche am Bonner Hauptbahnhof – in Deutschland in der Lage sein, solche Informationsmengen, die durch die Bevölkerung über Fahndungsaufrufe elektronisch übermittelt werden, zu bearbeiten. Das wird eine Herausforderung sein – für alle. Eine entsprechende Größenordnung lässt sich nur durch eine enge Zusammenarbeit von Bund und Ländern in Form einer Aufrufeinheit von ausgebildeten Videoanalysten und einer gemeinsam genutzten Infrastruktur realisieren.

Zusätzlich müssen die technischen Voraussetzungen für die Datenaufbereitung geschaffen werden: Derzeit gibt es noch keine Analyse- und Auswertetools zur automatisierten Bearbeitung von Foto- und Videodaten verschiedenster Formate. Bund und Länder sind aktuell dabei, Lösungen zu finden.

Der Anschlag in Boston zeigt darüber hinaus noch etwas anderes: Dass die polizeiliche Krisenkommunikation und taktische Öffentlichkeitsarbeit an das veränderte Kommunikationsverhalten der Bevölkerung angepasst werden muss. Der Gefahr von selbst ernannten Fahndern im Internet, die vermeintlich Verdächtige an den Pranger stellen, muss die Polizei mit deeskalierender Öffentlichkeitsarbeit im Internet begegnen. Klassische Medien müssen mit den interaktiven Möglichkeiten des WEB 2.0 und deren mobilen Nutzung kombiniert werden.

Es ist selbstredend, dass die Verlagerung der Kriminalität in die digitale Welt, strukturelle Anpassungen erfordert. Polizeibehörden benötigen professionelle und zukunftsorientierte Ausrichtungen.

In diesem Jahr haben wir im Bundeskriminalamt einen neuen Kompetenzbereich aufgebaut, der ausschließlich Cybercrime bekämpft. Dabei war für uns entscheidend, ermittlungsunterstützende Auswertung mit operativen Ermittlungen organisatorisch eng zu verknüpfen. Über 150 Spezialisten sollen Cyberkriminelle verfolgen, strafbares Handeln dokumentieren, erwirtschaftete Gewinne aufspüren und Vermögen abschöpfen.

Das für die erfolgreiche Bekämpfung von Cybercrime erforderliche Know-how bauen wir unter anderem durch den Einsatz von Cyberanalysten weiter aus. Diese IT-Experten werden im Team mit Kriminalbeamten in der Fallbearbeitung eingesetzt. Von dieser sogenannten „Tandem-Lösung“ erwarten wir zugleich eine Stärkung einschlägiger Fachkenntnisse bei allen Teammitgliedern.

Das Internet als Tatmittel ist inzwischen allgegenwärtig. Deshalb brauchen wir spezifische IuK-Kompetenzen auch in anderen Phänomenbereichen, z.B. zur Bekämpfung der digitalen Verbreitung von Kinderpornographie als besonders widerwärtiger Form eines durch die Spezifika des Verbreitungsmediums auf Dauer dokumentierten Kindesmissbrauchs, des Rauschgifthandels, aber eben auch im Bereich der Spionage, der nachrichtendienstlich gesteuerten Angriffe auf kritische Infrastrukturen sowie beim Extremismus und Terrorismus.

Für extremistische und terroristische Organisationen und Gruppierungen ist das Internet das wichtigste Mittel zur Verbreitung von Propaganda und unterschiedlichsten Handlungsanleitungen. Das Gemeinsame Internetzentrum wie auch die Koordinierte Internetauswertung im rechten und linke Extremismusbereich versetzen uns in die Lage, Kommunikationswege von Straftätern, Strukturen, Abläufe, Anschlagsplanungen und sonstige phänomenbezogene Verhaltensweisen frühzeitig zu erkennen und zu bewerten.

Im Phänomenbereich der Cyberspionage sind in Deutschland ausländische Nachrichtendienste unvermindert tätig – nicht erst die aktuellen Debatten legen diesen Fakt offen.

IT-Angriffe mittels Hacking und Malware sind grundsätzlich von jedem Ort der Welt aus und zu jeder Tages- und Nachtzeit möglich. Ernsthafte strafrechtliche Risiken bestehen für die Angreifer kaum, da IT-Angriffe von Nachrichtendiensten dem äußeren Anschein nach nur schwer von allgemeinkriminellen IT-Angriffen zu unterscheiden und die ND-Täter in ihrem Heimatland vor Strafverfolgung weitgehend geschützt sind.

Wir werden uns durch die Einrichtung eines Arbeitsbereiches Cyberspionage in der Abteilung Polizeilicher Staatsschutz des BKA auch dieser Herausforderung verstärkt annehmen.

Alle Konzepte und Strategien fruchten nicht ohne geeignete, fachkundig ausgebildete Mitarbeiterinnen und Mitarbeiter in den Sicherheitsbehörden und bei der Justiz.

Bereits seit dem Jahre 2006 setzen wir im BKA intensiv das gemeinsam mit den Ländern erarbeitete IuK-Fortbildungskonzept um.

Da am Ende der Prozesskette die Verurteilung des Straftäters für die verübten Taten stehen muss, ist es wichtig, bei Investitionen in den personellen und fachlichen Kompetenzausbau den gesamten Funktionszusammenhang zwischen Polizei, Staatsanwaltschaft und Gerichte im Blick zu haben. Polizeiliche Ermittlungsarbeit ist kein Selbstzweck! Auch die Justiz muss entsprechend aufgestellt sein, sonst produziert die Polizei einen enormen Input an Verfahren und die Justiz ebenso hohe Einstellungsquoten.

Der Aufbau von Expertise bei der Justiz über die Einrichtung von Schwerpunktstaatsanwaltschaften wie die "Zentralstelle zur Bekämpfung der Internetkriminalität" der Generalstaatsanwaltschaft Frankfurt (Main) sind daher Maßnahmen, die unabdingbar sind, wenn wir dem Phänomen jetzt und in Zukunft effektiv begegnen wollen.

Die polizeiliche und justizielle Expertise reicht jedoch allein nicht aus. Um den genannten Bedrohungen zu begegnen, ist eine Ausweitung der Abwehrbemühungen über den Schutz der staatlichen Netze hinaus erforderlich.

Wertvolle Erkenntnisse zu modi operandi, aber auch unverzichtbares Know-how liegen nicht nur bei staatlichen Akteuren, sondern in wissenschaftlichen Einrichtungen und Wirtschaftsunternehmen, insbesondere in den Unternehmen der IT-Branche, die zum Teil erhebliche Ressourcen in Analyse und Sicherheit investieren.

Infrastrukturprovider, Serviceprovider, Contentprovider – private Unternehmen sind wesentliche Akteure bei Auf- und Ausbau, Betrieb und Weiterentwicklung des Internet und der darüber angebotenen Produkte und Dienstleistungen. Gleiches gilt für die Bereiche Hard- und Softwareentwicklung.

Unternehmen können durch ein der Bedrohungslage angemessenes Verhalten einen Beitrag leisten – insbesondere im präventiven Bereich. Beispielsweise durch Einhaltung von Mindeststandards zur IT-Sicherheit.

Darüber hinaus verfügen Unternehmen bei Cyberangriffen über wichtige Informationen für die Polizei. Studien belegen: Unternehmen zeigen Angriffe nur selten an – trotz aller Sensibilisierungsbemühungen der Sicherheitsbehörden.

Der Aufwand einer Anzeige sei zu hoch, der Ermittlungserfolg der Behörden demgegenüber zu unwahrscheinlich, richtige Ansprechpartner auf Seiten der Behörden seien nicht bekannt. Es kommt noch ein weiterer Grund hinzu: der befürchtete Ansehensverlust.

So nachvollziehbar diese Begründungen auf den ersten Blick erscheinen, so kontraproduktiv sind die Folgen für die Gemeinschaft: Solange Unternehmen erkannte Angriffe verschweigen, gibt es keinen Ermittlungsansatz für die zuständigen Behörden und damit keinen validen Überblick über die gesamte Bedrohungslage. Die Schadenspotenziale vergrößern sich durch Nichtanzeige!

Mit Zusammenarbeit meinen wir aber nicht nur das Stellen einer Strafanzeige. Zu einem ganzheitlichen Ansatz der Bekämpfung von Cybercrime gehört auch, die in Wirtschaft und Wissenschaft, in Unternehmen und an Forschungsinstituten vorhandene Fachkompetenz mit den polizeilichen Kompetenzen zu bündeln.

Hierzu möchte ich Ihnen zwei Vorhaben des BKA kurz vorstellen:

1. Je nach Angriffsstruktur – beispielsweise denke ich hier an speziell entwickelte Schadprogramme – kann es erforderlich sein, externe Spezialisten mit dem entsprechenden Fachwissen in den Bereichen Programmcode oder Netzwerkforensik hinzuzuziehen. Wir stellen uns hier das Modell einer Aufrufeinheit, einer so genannten „Quick Reaction Force Cybercrime“, bestehend aus Experten der Sicherheitsbehörden von Bund und Ländern, Spezialisten aus der Wirtschaft und Wissenschaft, vor. Die Einrichtung einer Aufrufeinheit würde die Reaktionsfähigkeit bei Eintritt eines Schadensfalles deutlich beschleunigen, da bereits bei Beginn der Ermittlungen die benötigte Expertise zur Verfügung steht.
2. Private und Polizei müssen sich gegenseitig in ihrer Arbeit unterstützen. Wir benötigen einen tagesaktuellen Austausch über Bedrohungen, Sicherheitsmaßnahmen und taktisch wichtige Informationen. Für den Phänomenbereich Cybercrime haben wir deshalb modellhaft und als ersten Schritt eine institutionalisierte Public Private Partnership mit zentralen Akteuren aus dem Bankensektor bereits geschlossen. Hiervon erhoffen wir uns eine Verkürzung der Kommunikationswege, die Bildung von Vertrauen und Verständnis für die Partner und einen effektiven Austausch der Erkenntnisse.

Unbestreitbar ist zudem das Erfordernis, dass Cybercrime im internationalen Verbund bekämpft werden muss. Das Bundeskriminalamt hat in den vergangenen Jahren ein internationales Netz der vertrauensvollen Zusammenarbeit mit Cybercrimedienststellen in aller Welt aufgebaut und wird dies unter Einbeziehung von Europol und Interpol weiter ausbauen.

Auch die Rechtsetzung muss an die Erscheinungsformen von Cybercrime angepasst werden – und zwar auf mehreren Ebenen. Dabei muss die Ungleichzeitigkeit von technologischer Entwicklung und der Reaktionszeit der Politik im Hinblick auf rechtliche Anpassungsnotwendigkeiten als besondere Herausforderung gesehen werden.

Sekundenschnelle Ortswechsel von Informationen über das Internet auf Server oder in Clouds rund um die Welt und die Flüchtigkeit digitaler Spuren kontrastieren mit starren rechtlichen Strukturen der internationalen Zusammenarbeit und den Bürokratismen der internationalen Rechtshilfe.

Wir benötigen daher eine multilaterale Verständigung über einen internationalen rechtlichen Rahmen, der uns die Strafverfolgung im Bereich der Cybercrime schneller und effizienter ermöglicht.

Neben der Harmonisierung des Strafrechts und dem Schließen von Strafbarkeitslücken müssen polizeiliche Eingriffsbefugnisse um Methoden, die den technologischen Entwicklungen entsprechen, technikoffen ergänzt werden.

Der Bundespräsident hat in seiner Rede zum Tag der deutschen Einheit die digitale Revolution als eine der großen Herausforderungen unserer Zeit herausgestellt.

Ich zitiere: „Wir befinden uns mitten in einem Epochenwechsel. Ähnlich wie einst die industrielle Revolution verändert heute die digitale Revolution unsere gesamte Lebens- und Arbeitswelt, das Verhältnis vom Bürger zum Staat, das Bild vom Ich und vom Anderen."

Genauso real wie die technologischen Fortschritte das Leben erleichtern ist unbestreitbar das damit einhergehende Missbrauchs- und Bedrohungspotenzial.

Die Frage nach informationeller Selbstbestimmung ist angesichts der für den Einzelnen kaum noch durchschaubaren Prozesse der Datenvernetzung und Datenverknüpfung einem diffusen Gefühl eines hinzunehmenden Ausgeliefertseins gewichen, das Vertrauen tendenziell untergräbt und Misstrauen fördert.

Die potenzielle Abtrennbarkeit eines digitalen von dem realen Selbst ist alles andere als eine positive Verheißung. Autonome Verfügbarkeit über das Identitätsprägende verliert so seine Selbstverständlichkeit.

Wegen ihrer Eingriffsbefugnisse war eine omnipräsente und omnipotente Polizei mit unserem Freiheitsverständnis noch nie vereinbar. In einer digitalen Welt ist sie es noch weniger.

Genauso wenig ist aber eine, trotz erkennbarer technologischer Entwicklungen, in ihren Instrumentarien zögerlich limitierte Polizei mit effektiver Verbrechensbekämpfung und Rechtssicherheit überein zu bringen.

Weil der Zweck des Rechts in der Stabilisierung von Verhaltenserwartungen und dem Aufbau von Vertrauen liegt, geht es um das Optimierungsgebot zwischen Abwehrrechten und Schutzpflichten, um die Balance zwischen Freiheit und Sicherheit. Im Kern ist die Frage nach der Legitimität unserer Rechtsordnung aufgeworfen, die auf Rechtsetzung und Rechtsdurchsetzung gründet und der vermeintlichen Differenz von analoger und digitaler Welt mit der Einheit der Rechtsordnung begegnet.

Es bedarf mehr denn je eines gesellschaftspolitischen und verfassungspolitischen Diskurses über Fragen der Menschenwürde und der Privatheit in einem digitalen Zeitalter. Auch eines Diskurses über das technisch Machbare und das normativ Wünschbare und Zulässige. Genauso eines Diskurses über den Ausbau des Grundrechtsschutzes durch entsprechende Kontrollverfahren.

Letztlich geht es um Vertrauen: In das Internet, in die Sicherheitsbehörden, in den Rechtsstaat, der seiner Schutzpflicht angemessen genügen muss. Pauschalierende Etiketten werden diesen diffizilen Themen und dem Bemühen um eine Antwort nicht gerecht.