Bernd Busemann Niedersächsischer Justizminister

Arbeitskreis Vorratsdatenspeicherung
Ortsgruppe Hannover
[redacted]

Hannover, den 28. Sep. 2012

- 4103 I – 404. 216 -

Offener Brief zum Thema Vorratsdatenspeicherung

Sehr geehrter Herr Ebeling,

auf Ihr Schreiben antworte ich auch im Namen des Leitenden Oberstaatsanwaltes in Hannover gerne, gibt mir dies doch Gelegenheit, mit einigen Missverständnissen aufzuräumen, zumal Sie zugesagt haben, mein Schreiben in voller Länge auf Ihrer Homepage einzustellen.

Die moderne Kommunikationstechnik hat heute in nahezu allen Lebensbereichen Einzug gehalten und beeinflusst die Gestaltung unseres Privat- und Berufslebens maßgeblich. Dies gilt selbstverständlich auch für diejenigen, die Informationstechnologien für kriminelle Zwecke nutzen bzw. missbrauchen. So hat die Veränderung der Kommunikationslandschaft u.a. zu völlig neuen Kriminalitätsformen geführt, wie z.B. dem so genannten „Phishing", bei dem zielgerichtet Bankdaten zum Zwecke des Zugriffs auf Konten von Bürgerinnen und Bürgern ausgespäht und manipuliert werden. Zum anderen verändern sich auch „altbekannte" Delikte durch die neuen Technologien, der Austausch kinderpornographischen Materials erfolgt gegenwärtig zu fast 100% über das Internet, sogenannte „Abofallen" haben die „Haustürgeschäfte" abgelöst. Ein persönlicher Täter - Opfer - Kontakt oder bei „Bandentaten"

Am Waterlooplatz 1
30169 Hannover
Telefon 0511 120-5069
Telefax 0511 120-5183
E-Mail bernd.busemann@

ein persönlicher Kontakt zwischen den häufig arbeitsteilig agierenden Mittätern ist „in der realen Welt" in vielen Fällen überhaupt nicht mehr erforderlich. Klassische polizeiliche Ermittlungsansätze, wie beispielsweise Fingerabdrücke, DNA-Profile oder „Phantomskizzen" ergeben sich dann nicht mehr und laufen zwangsläufig ins Leere.

Diese durch die technische Entwicklung bedingte Veränderung unseres Kommunikationsverhaltens, die zwangsläufig andere Ermittlungsansätze bedingt, war der Grund für die EU-Richtlinie, in deren Umsetzung die so genannte Vorratsdatenspeicherung in den europäischen Staaten eingeführt wurde.

Bei den zu speichernden Daten, den „Vorratsdaten" oder korrekt „Verkehrsdaten im Bereich der Telekommunikation" handelt es sich – im Gegensatz zu den Kommunikationsinhalten – um Nutzungsdaten, wie

1. die Rufnummern,
2. Zeit und Dauer der Verbindung,
3. Art des genutzten Dienstes,
4. die Bezeichnung der bei Beginn der Verbindung genutzten Funkzellen (Standorte) der
5. Internetprotokolladressen (IP-Adressen), Kennung der beteiligten Anschlüsse, sowie Zeit und Dauer der Internetverbindung.

Es handelt sich also nicht um die Inhalte von Telefonaten, E-Mails oder Internetseiten, sondern ausschließlich um reine Nutzungsdaten, die Aufschluss darüber geben, wann, wo, wie oft und wie lange ein bestimmter Verbindungsweg genutzt wurde. Diese Daten wurden seit dem 01.01.2008 von den Betreibern durch Speicherung vorrätig gehalten.

Mit dem Urteil des Bundesverfassungsgerichts vom 02.03.2010 sind die als „Vorratsdaten" gespeicherten Telekommunikationsverkehrsdaten ersatzlos weggefallen.

Die Entscheidung des Bundesverfassungsgerichts stellt die Strafverfolgung vor erhebliche Probleme. Einerseits sind die Strafverfolgungsbehörden an ihren verfassungsrechtlichen Auftrag gebunden, im Interesse des Gemeinwohls eine effektive Strafverfolgung sicherzustellen. Andererseits sind durch den Wegfall der Vorratsdaten erhebliche Schutzlücken entstanden. Staatsanwaltschaft und Polizei können bei ihren Ermittlungen nun nur noch auf diejenigen Verbindungsdaten zurückgreifen, die die Unternehmen gem. § 96 TKG für ihre betrieblichen Zwecke, also in der Regel zu Abrechnungszwecken, speichern. Der wesentliche Unterschied zur vorsorglichen Datenspeicherung nach § 113a TKG besteht darin, dass die Unternehmen jetzt nicht mehr verpflichtet sind, überhaupt Daten zu speichern. Sie haben lediglich das Recht dazu (§ 96 Abs.1 TKG). Die betrieblichen Zwecke, für die die Speicherung erfolgt, unterschieden sich zudem nicht nur von Unternehmen zu Unternehmen, sondern auch von Vertrag zu Vertrag. Sie richten sich beispielsweise nach der Vertragsgestaltung oder danach, welche Daten das Unternehmen für seine Verwaltung und Geschäftspolitik benötigt. Ob und welche Daten daher auf der Grundlage eines richterlichen Beschlusses z.B. nach § 100g Abs.1 StPO erlangt werden können, ist damit seit der Entscheidung des Bundesverfassungsgerichts nur noch von Zufälligkeiten abhängig.

Für die Strafverfolgung und für die Abwehr erheblicher Gefahren im Bereich des Terrorismus und der Organisierten Kriminalität sowie in Deliktsfeldern wie der Kinderpornografie ist die Vorhaltung von Telekommunikationsverkehrsdaten über einen gewissen Mindestzeitraum von essentieller Bedeutung. Gerade konspirativ vorgehende Tätergruppen bedienen sich zunehmend der neuen Informations-/ Kommunikationstechnologien. So wird beispielsweise der groß angelegte „Drogendeal", bei dem Rauschgift im Kilobereich aus dem Ausland eingeführt wird, heute vor dem eigentlichen Übergabetermin detailliert via Email-Verkehr abgestimmt. Die Weitergabe von kinderpornografischen Schriften erfolgt nicht mehr wie früher in

dunklen Hinterhöfen, sondern über Chatrooms im Internet. Kann man dann die IP-Adressen der „User" mangels Speicherung nicht mehr ermitteln, sind dem ungehemmten Handel mit kinderpornografischen Schriften Tür und Tor geöffnet. Dies ist im konkreten Fall gerade deshalb so fatal, weil hinter jedem kinderpornografischen Bild der reale sexuelle Missbrauch eines Kindes steckt.

Für die Strafverfolgungsbehörden ist daher die gesetzliche Regelung der Speicherpflichten und -fristen zwingend erforderlich. Eine erfolgreiche Ermittlungsführung ist mittlerweile in vielen, gerade die schwere Kriminalität betreffenden Fällen nicht mehr möglich, weil die Verkehrsdaten als wesentliche Ermittlungsansätze nicht (mehr) zur Verfügung stehen.

Das Bundesverfassungsgericht hat entgegen anderslautender Behauptungen die „Vorratsdatenspeicherung" allerdings nicht an sich für verfassungswidrig erklärt. Im Gegenteil: Das Bundesverfassungsgericht hält eine Neuregelung ausdrücklich für möglich und zulässig. Erforderlich sei jedoch, dass hinreichend anspruchsvoll und normenklar die Voraussetzungen im Hinblick auf die Datensicherheit, die Anlässe und Zwecke der Datenverwendung (d. h. Eingriffsschwellen), die Transparenz (d. h. Erkennbarkeit für den Betroffenen) und den Rechtsschutz des Betroffenen festgelegt werden. Die Richtlinie der EU 2006/24/EG, die die Anbieter von Telekommunikationsdiensten dazu verpflichtet, die in § 113a TKG erfassten Daten für mindestens 6 Monate und höchstens 2 Jahre zu speichern und für die Verfolgung von schweren Straftaten bereitzuhalten, kann daher verfassungskonform umgesetzt werden. Effektive Strafverfolgung in den von mir aufgezeigten Bereichen ist also nicht eine Frage des rechtlichen Könnens, sondern allein eine Frage des Wollens.

Der Staat kann es sich auf Dauer nicht leisten, den Schutz der Bevölkerung vor hochkriminellen Tätern zu vernachlässigen. In dem Maße wie der Staat hier seinen Pflichten nicht nachkommen kann, wird sich die Nutzung neuer Kommunikationstechnologien zu immer ausgefeilteren Straftaten erhöhen.

Dies vorangestellt, beantworte ich Ihre Fragen wie folgt:

1. Die Zahlen, die anlässlich der Pressekonferenz von mir, Herrn Generalstaatsanwalt in Celle sowie dem Leitenden Oberstaatsanwalt in Hannover genannt worden sind, entstammen der internen Statistik der Zentralstelle zur Bekämpfung gewaltdarstellender, pornographischer oder sonst jugendgefährdender Schriften bei der Staatsanwaltschaft Hannover. Diese hat im Jahr 2007 und 2008 jeweils etwa 4000 Verfahren, 2009 3271 Verfahren und im Jahr 2010 nur noch 1902 sowie 2011 ebenfalls knapp 2000 Verfahren eingeleitet, die in ihre Zuständigkeit fallen.
   Bereits deswegen können diese Zahlen nicht mit denen von Minister Schünemann genannten Zahlen, die sich ausschließlich auf den „Handel mit kinderpornographischen Material" bezogen, übereinstimmen; sie entstammen unterschiedlichen Statistiken. Beide Statistiken zeigen jedoch einen erheblichen Rückgang dieses Deliktsfeldes auf.

   Mein Kollege Schünemann hat anlässlich der Präsentation der Polizeilichen Kriminalstatistik hinsichtlich des Deliktsfeldes Kinderpornographie generell ausgeführt, dass die Verbreitung kinderpornographischen Materials über das Internet erfolge. Innenminister Schünemann machte diesbezüglich unmissverständlich deutlich: „Die Aufklärungsquote ist in diesen Fällen im vergangenen Jahr bereits unter 70 Prozent gesunken, im Jahr 2009 betrug sie noch 82,25 Prozent, im Jahr 2010 waren es 75,53 Prozent. Das erneute Absinken der Aufklärungsquote in Niedersachsen um etwa 5 Prozent bei der Verbreitung von Kinderpornografie unter Nutzung des Tatmittels Internet unterstreicht die Problematik der fehlenden Vorratsdatenspeicherung[1]"

[1] PI des Niedersächsischen Ministerium für Inneres und Sport vom 15.02.2012

Eine unterschiedliche Darstellung bzw. unterschiedliche Tendenzen kann ich hierin nicht erkennen. Mein Kollege und ich haben anhand der Erhebungen festgestellt, dass der Wegfall der Vorratsdatenspeicherung erhebliche negative Auswirkungen auf die Verfolgung der Kinderpornographie hat.

2. Bei der Verfolgung von Internetkriminalität stellt regelmäßig die IP-Adresse des Täters den einzigen Ermittlungsansatz dar. Zur Ermittlung der einer dynamischen IP zuzuordnenden Bestandsdaten müssen die Netzbetreiber auf Verkehrsdaten, die sog. Log-Files, zurückgreifen. Nach dem Wegfall der Vorratsdatenspeicherung werden diese Daten - mangels betrieblicher Speichererfordernisse - nicht mehr oder nur noch wenige Tage gespeichert. Eine retrograde Ermittlung des Nutzers einer bestimmten IP ist daher regelmäßig nicht mehr möglich. Der Wegfall der Vorratsdatenspeicherung betrifft daher insbesondere Verfahren wegen Verbreitung, Erwerbs und Besitzes kinder- und jugendpornographischer Schriften gemäß §§ 184b und c StGB. Ihre Ansicht, dass das „Bekanntwerden von Internetstraftaten" nicht vom Wegfall der Vorratsdatenspeicherung beeinflusst wird, ist falsch.

Zum einen ist den Rechteverwertern der Wegfall der Vorratsdatenspeicherung und deren Auswirkung auf die Ermittlungsmöglichkeiten bekannt; wegen Aussichtslosigkeit verzichten sie bereits auf Strafanzeigen; scheinbar nehmen die Straftaten ab, tatsächlich erfolgt lediglich eine Verschiebung ins Dunkelfeld. Zum zweiten werden aufgrund der fehlenden Vorratsdatenspeicherung Listen mit IP-Adressen, die zum Beispiel im Rahmen der Auswertung eines beschlagnahmten Computers erstellt werden könnten und grundsätzlich belegen, dass ein Austausch von kinderpornographischem Material stattgefunden hat, nicht mehr weiter ausgewertet. Insofern liegt keine „Behinderung der Ermittlungen"

vor, es werden schlichtweg keine Verfahren mehr eingeleitet, weil von Anfang an klar ist, dass es keinen zu Erfolgen führenden Ermittlungsansatz gibt. Um es deutlich zu sagen: Hier wird durch die fehlende Vorratsdatenspeicherung bereits die Einleitung eines Ermittlungsverfahrens verhindert, was dazu führt, dass die „sichtbare" Kriminalität abnimmt. Der unkundige Laie könnte versucht sein zu glauben, die Straftaten in diesem Bereich gingen tatsächlich zurück. Dies ist jedoch nicht der Fall; die Kriminalität wird in das Dunkelfeld verschoben.

3. Die Ermittlungsbehörden sind tagtäglich damit konfrontiert, dass z.B. bei der Auswertung eines sichergestellten Computers zahlreiche IP-Adressen festgestellt werden, von denen ein Austausch inkriminierten Materials begangen wurde. Neue Verfahren werden jedoch nicht eingeleitet, weil von vornherein feststeht, dass sich ein Beschuldigter nicht ermitteln lassen wird. Große bundesweite Ermittlungen, wie z.B. die Operation „Himmel" im Jahr 2008, werden seit Wegfall der Vorratsdatenspeicherung nicht mehr geführt. So konnten vor einiger Zeit in einem Ermittlungskomplex zwar 15.000 IP-Adressen festgestellt werden, von denen kinderpornographisches Material verschafft worden war. Vor Wegfall der Vorratsdatenspeicherung hätte man aber die hinter den IP-Adressen stehenden Nutzer festgestellt und eine entsprechende Anzahl von Ermittlungsverfahren gegen Beschuldigte im In- und Ausland einleiten können. Wegen des Wegfalls der Vorratsdatenspeicherung konnten nur noch 200 IP-Adressen konkreten Personen zugeordnet werden. Das bedeutet: Nur in 1,3 % wurden tatsächlich Verfahren eingeleitet. Bei den übrigen 98,7 % konnte nicht einmal ansatzweise versucht werden, die Straftaten zu verfolgen, geschweige denn zu sühnen.

4. Die Strafverfolgungsbehörden sind an ihren verfassungsrechtlichen Auftrag gebunden, im Interesse des Gemeinwohls eine effektive Strafverfolgung sicherzustellen, unabhängig davon, ob diese Straftaten im, mit Hilfe des oder ohne das Internet begangen werden.

Diesem Auftrag stellen sich die Strafverfolgungsbehörden seit vielen Jahren mit großem Engagement. Sofern es Defizite in der Strafverfolgung gibt, suchen die Strafverfolgungsbehörden nach Verbesserungsmöglichkeiten, sei es durch Aus- und Fortbildung, Ergänzung der Ausstattung oder Umstrukturierung. Sofern das Defizit im rechtlichen Bereich liegt, ist es Aufgabe des Gesetzgebers, diesen Mangel durch gesetzgeberische Maßnahmen zu beenden. Stellt sich der Gesetzgeber seiner Aufgabe nicht, so müssen ihn die Strafverfolgungsbehörden darauf hinweisen, dass sie ihrem verfassungsrechtlichen Auftrag unter diesen Umständen nicht nachkommen können. Dass mein Engagement für die Einführung der Vorratsdatenspeicherung, die sowohl aus europarechtlicher aber eben auch aus tatsächlicher Hinsicht, dringend notwendig ist, dazu führen könnte, dass andere Straftaten nicht angemessen verfolgt würden, ist grotesk. Es ist meine Aufgabe als Justizminister, das Petitum u.a. meines Geschäftsbereiches deutlich zu machen, wenn sich der Bundesgesetzgeber seit Jahren weigert, seine Hausaufgaben zu machen und dies dazu führt, dass Strafverfolgung bzgl. bestimmter Straftaten nicht mehr möglich ist.

5. Auch in Fällen des „Enkeltricks" erweist sich der Wegfall der Vorratsdatenspeicherung regelmäßig als erhebliches Ermittlungshindernis. In diesen Fällen – es handelt sich um organisierte Kriminalität – werden von den Tätergruppen zumeist ältere Personen auf ihrem Festnetzanschluss angerufen. Nach Vorspiegelung eines Verwandtschaftsverhältnisses und Schilderung einer akuten Notlage bittet der Anrufer um die kurzfristige Überlassung einer größeren Geldsumme. Die Opfer werden hierbei von den professionellen Tätern derart unter Druck gesetzt, dass sie sich dieser „Bitte" häufig nicht entziehen können. Dieser Betrag – bei dem es sich in der Regel um sämtliche Ersparnisse des Opfers handelt - wird in der Folge durch einen der Täter bei dem Opfer persönlich abgeholt. Auch in diesen Fällen stellt die Nummer des Anrufers in der ganz überwiegenden Anzahl der Fälle den einzigen Ermittlungsansatz dar. Da die Daten, wenn überhaupt, nur für wenige Tage gespeichert werden, die Strafanzeige

durch das Opfer indes oft erst mehrere Tage nach der Tat erfolgt, müssen die Ermittlungen eingestellt.

Trotz der verharmlosenden Bezeichnung „Enkeltrick" handelt es sich – anders als Sie meinen - hierbei nicht um eine Bagatelltat, sondern um eine schwere Straftat im Sinne des § 100g StPO: Ungeachtet dessen, dass die Täter ihre Opfer regelmäßig finanziell vollständig ruinieren, erfolgt der „Enkeltrick" nach Erkenntnissen der Strafverfolgungsbehörden durch eine straff gegliederte Täterorganisation, die nicht nur bundes-, sondern europaweit agiert.

Der „Enkeltrick" wird ausschließlich von perfekt durchorganisierten Angehörigen einer ethnischen Minderheit, die nicht ortsgebunden und deshalb schon schwer zu verfolgen sind, begangen. Seit geraumer Zeit haben diese wegen des erhöhten Verfolgungsdruckes in Deutschland ihr Lager in Osteuropa bezogen, von wo aus derzeit die Taten gesteuert werden. So schwärmen jeweils zum Wochenbeginn die Geldabholer heuschreckengleich zu vorher von den Köpfen der Bande festgelegten Zielen in Deutschland, der Schweiz und Österreich aus. Nach der Ankunft am jeweiligen Zielort erfolgen dann die Anrufe von psychologisch bestens geschulten Bandenmitgliedern aus Osteuropa bei den potentiellen Opfern, die idR um nahezu ihre gesamten Ersparnisse gebracht werden.

Strafrechtlich handelt es sich nicht nur um (eine Vielzahl von Fällen des) besonders schweren Fall des Betruges, der mit Freiheitsstrafe bis zu 10 Jahren bestraft werden kann (§ 263 Abs. 3 Nr. 1 StGB), sondern um ein qualifiziertes Verbrechen, mit einer Mindestfreiheitsstrafe von einem Jahr (§ 263 Abs. 5 StGB).

Die meisten Tatbeteiligten, insbesondere die Drahtzieher und Organisatoren halten sich im Hintergrund. Das größte Entdeckungsrisiko und das Risiko einer

Festnahme tragen die Geldabholer, die mit den Opfern der Taten in unmittelbaren Kontakt treten. Zur Bekämpfung dieses Kriminalitätsfeldes ist es besonders wichtig, sich nicht nur mit den austauschbaren Randfiguren zu befassen, sondern die Organisatoren und Profiteure zu ermitteln und ihnen das Handwerk zu legen.
Die Ermittlungen der Organisationsstrukturen und der Hinterleute ist entscheidend davon abhängig, dass die Telekommunikation zwischen Tätern und Opfern sowie zwischen den verschiedenen Tatbeteiligten nachvollzogen werden kann. Hierzu benötigen die Ermittlungsbehörden insbesondere die Feststellung von Verbindungsdaten, die im Zusammenhang mit Telefonaten anlässlich der Tatbegehung in der Vergangenheit angefallen sind. Gerade aus deren Analyse lassen sich oft die entscheidenden Indizien für die Überführung der einzelnen Tatbeteiligten ableiten.

Das strafprozessuale Instrumentarium zur Erhebung dieser Daten ist vorhanden. Allerdings scheitert die Erhebung der Verbindungsdaten an der fehlenden Vorratsdatenspeicherung.

Die Ermittlung der gut verdienenden Hintermänner unterbleibt.

Dies gilt im übrigen auch für den gesamten Bereich der organisierten Kriminalität, denn diese Art der Kriminalität lebt von der schnellen Kommunikation zur gemeinsamen Planung und arbeitsteiligen Begehung schwerer Straftaten. Durch die zum Teil nur kurzen Speicherfristen besteht insbesondere die Gefahr, dass aus der Auswertung retrograder Verkehrsdaten sich erschließende Zusammenhänge zwischen Einzeltaten, z.B. bei Serieneinbrüchen „reisender" Tätergruppierungen, nicht erkannt und damit auch die hinter den Einzeltätern agierenden hauptverantwortlichen (OK-) Täter nicht mehr identifiziert und verfolgt werden.

Die niedersächsische Polizei hat für den Zeitraum vom Juli 2010 bis September 2012 eine interne Erhebung durchgeführt. Diese ergab, dass bei den – für diesem Zeitraum - 1447 gemeldeten Straftaten, in denen es aus Ermittlungsgründen erforderlich gewesen wäre, die Verbindungsdaten zu erheben, 1344 Taten gar nicht mehr bzw. nur noch unzureichend aufgeklärt werden konnten. Dieser Umstand belegt, dass für eine Vielzahl von Straftaten Verkehrsdaten den einzigen Ermittlungsansatz darstellen und nach Wegfall der so genannten Vorratsdatenspeicherung nicht mehr bzw. nur wesentlich erschwert aufgeklärt werden können. Nur der Vollständigkeit halber weise ich darauf hin, dass Verkehrsdaten im Rahmen eines Strafverfahrens nicht nur belastend, sondern auch entlastend sein können.

Mit freundlichen Grüßen

[redacted]

Bernd Busemann