

Die Fälle, in denen das Internet als Hilfsmittel zur Begehung von Straftaten verwendet wird, steigen stetig und exponentiell schnell an. In der polizeilichen Kriminalstatistik ist ein Zuwachs von ca. 20 Prozent beim Vergleich der Jahre 2009 und 2010 zu verzeichnen. Zahlen für 2011 liegen zwar noch nicht vor, ein weiterer deutlicher Anstieg gilt unter Experten allerdings als sicher. Eine erfolgreiche Ermittlungstätigkeit in diesen Fällen setzt sowohl bei der Polizei als auch den Staatsanwaltschaften Fähigkeiten und Kenntnisse voraus, die bis vor kurzem weder in der juristischen noch in der polizeilichen Ausbildung eine den sich stellenden Heraus-

forderungen entsprechende Rolle gespielt haben: ein vertieftes, über reines Anwenderwissen hinausgehendes Verständnis für IT-Sachverhalte. Selbstverständlich dürfen auch die damit einhergehenden (grund-)rechtlichen Implikationen, die sich – Beispiel: Staatstrojaner – nur erschließen, wenn ein technisches Grundverständnis vorhanden ist, nicht zu kurz kommen.



Professor
Dr. Jan Dirk Roggenkamp,
Berlin/Nienburg (Weser)

Schutz und Sicherheit in der virtuellen Welt

forderungen entsprechende Rolle gespielt haben: ein vertieftes, über reines Anwenderwissen hinausgehendes Verständnis für IT-Sachverhalte. Selbstverständlich dürfen auch die damit einhergehenden (grund-)rechtlichen Implikationen, die sich – Beispiel: Staatstrojaner – nur erschließen, wenn ein technisches Grundverständnis vorhanden ist, nicht zu kurz kommen.

Anfang Januar verkündete der Bayerische Innenminister *Hermann*, dass in Bayern 54 sogenannte Internetpolizisten, also Computer- und Informatik-Experten, die zusätzlich zu Vollzugsbeamten ausgebildet worden sind, ihren Dienst beginnen werden. Auch wenn es sich *Hermann* nicht nehmen ließ, in diesem Kontext die Phrase „Das Internet darf kein rechtsfreier Raum sein“¹ zu dreschen, ist dieser Ansatz ein überzeugender. Weniger überzeugend als die fast schon poetisch anmutende Feststellung „Am virtuellen Tatort hilft kein Fingerabdruckpulver“ fällt die – ebenfalls vorhersehbare – Schelte der Bundesjustizministerin mit Blick auf die fehlende Regelung der Vorratsdatenspeicherung (VDS) aus. *Hermann* meint, es sei „beschämend“, dass „ausgerechnet Deutschland“ hier „im Hintertreffen“ sei. Diese Einschätzung ist nur schwer nachvollziehbar. Sicherlich mag es misslich sein, wenn sich die Spur eines Täters im Internet verliert. Ob allerdings die VDS hier das Allheilmittel ist, als das es immer wieder dargestellt wird, harret weiterhin eines substantiierten Nachweises. Fakten für das Gegenteil sind hingegen Legion: so kann beispielsweise die IP-Adresse eines UMTS-Internetzugangs (Internetstick, Smartphone), eines Rechners im Internet-Café oder eines Hotspots keiner bestimmten Person zugeordnet werden. Die VDS liefe leer. Auch die Verbreitung von statischen IPv6-Adressen wird den „Bedarf“ weiter verringern.

Das BVerfG hat die anlasslose Datenspeicherung in ihrer ursprünglich geplanten Form als besonders schweren Eingriff eingestuft, der eine Streubreite aufweise, den die Rechtsord-

wendig (und sinnvoll) erachten wollte, ein großes Maß an gesetzgeberischem Feingefühl erforderlich, um die umfassenden verfassungsrechtlichen Vorgaben des BVerfG zu erfüllen. Keinesfalls wird die VDS dazu dienen können, die „normale“ IT-gestützte Kriminalität zu bekämpfen. Eine Verwendung käme nur für „überragend wichtige Aufgaben des Rechtsgüterschutzes“ in Betracht. Ein Mehr an Sicherheit könnte im Gros der Fälle nicht gewährleistet werden.

Sinnvoller und schon heute erfolgreich ist die aktive Nutzung sozialer Netzwerke durch die Polizei. Hier hat sich insbesondere ein Pilotprojekt der Polizei Hannover zur Fahndung nach Tätern und vermissten Personen über eine Facebook-Fanseite² als effektive Maßnahme erwiesen. Die per virtuellem Steckbrief Gesuchten konnten, dank „Teilen“-Funktion und mit Hilfe der über 95 000 „Fans“, teilweise bereits nach wenigen Stunden gefunden werden. Auch in Bayern, Baden-Württemberg, Nordrhein-Westfalen und Brandenburg wird Presseberichten zufolge die Nutzung von Facebook, Twitter und Google+ erwogen. Nicht nur die Fahndung und Vermisstensuche, auch Öffentlichkeitsarbeit und Straftatenprävention über und mit Hilfe von Web 2.0-Plattformen ist angedacht. Die Reaktionen der Facebook-Fans sind positiv, die der Datenschutzbehörden bestenfalls verhalten.³ Der bayerische Datenschutzbeauftragte *Petri* hat indes eine erste Tendenz erkennen lassen: „Im Bereich der Gefahrenabwehr geht es unter Umständen um Leben und Tod. Ich werde den Innenminister nicht kritisieren, weil er eine Fahndung nach einem vermissten Kind bei Facebook einstellt.“⁴

1 Alle Zitate nach heise.de Meldung „Bayerische Internetpolizisten sollen Kriminalität im Netz bekämpfen“ v. 3. 1. 2012.

2 <http://de-de.facebook.com/PolizeiHannover>.

3 Z. B. in NRW: Siehe „Datenschutz – NRW-Polizei verschläft mögliche Fahndungserfolge per Facebook“ – DerWesten.de v. 6. 1. 2012.

4 Zitiert nach Schröpf, „Facebook-Cops sollen in Bayern Verbrecher jagen“ – Mittelbayerische Zeitung v. 10. 1. 2012.