**Bayerischer Landtag**
16. Wahlperiode

Drucksache 16/**8125**

29.04.2011

# Schriftliche Anfrage

der Abgeordneten **Susanna Tausendfreund**
**BÜNDNIS 90/DIE GRÜNEN**
vom 17.02.2011

**Rechtswidrige Computerüberwachung durch das LKA**

In der aktuellen Presseberichterstattung (z. B. Heise-Online vom 31.01.2011, Münchner Merkur vom 17.02.2011) wurde über den Beschluss des Landgerichts Landshut vom 20.01.2011, der im Rahmen eines Ermittlungsverfahrens (Az.: 4 Qs 346/10) gefasst wurde, berichtet. Danach war eine umfangreiche Überwachungsmaßnahme durch das LKA rechtswidrig, soweit grafische Bildschirminhalte (Screenshots) kopiert und gespeichert wurden. Diese Screenshots wurden im Rahmen einer am 02.04.2009 vom Amtsgericht gemäß § 100 a StPO angeordneten Überwachung und Aufzeichnung des Telekommunikationsverkehrs auf dem Computer des Beschuldigten gefertigt. Die Überwachungsanordnung bezog sich zwar auch auf die verschlüsselte Internetkommunikation über HTTPS und die verschlüsselte Internettelefonie wie Skype. Ausdrücklich unzulässig war jedoch die Onlinedurchsuchung des Computers, soweit es sich nicht um Telekommunikation handelte. Dennoch wurden vom LKA mithilfe eines installierten Trojaners rechtswidrig alle 30 Sekunden Bildschirmfotos des Browserinhalts erstellt und über 60.000 Bilder an die Behörde übertragen.

Ich frage die Bayerische Staatsregierung:

1. Aus welchen Gründen wurde die Anordnung des Amtsgerichts vom 02.09.2009 überschritten und damit missachtet?

2. Wer zeichnet für die Art und Weise der Durchführung dieser Maßnahme verantwortlich?

3. Gibt es interne Vorgaben, welche Maßnahmen die Überwachung und Aufzeichnung des Telekommunikationsverkehrs im repressiven und im präventiven Bereich umfassen und welche darüber hinausgehen?
   a) Wenn ja, wie lauten diese?

4. Gab es seit 2005 bzw. gibt es aktuell weitere Fälle, bei denen bei einer angeordneten Überwachung und Aufzeichnung des Telekommunikationsverkehrs Screenshots erstellt wurden?
   a) Wenn ja, wie viele?
   b) Wie viele Aufnahmen der Bildschirmoberfläche wurden jeweils erstellt und an die Ermittlungsbehörde übermittelt?

# Antwort

**des Staatsministeriums der Justiz und für Verbraucherschutz**
vom 25.03.2011

Die Schriftliche Anfrage beantworte ich im Einvernehmen mit dem Staatsministerium des Innern wie folgt:

Zu 1.:
In dem Ermittlungsverfahren war durch eine bereits laufende Telefonüberwachung festgestellt worden, dass sich die Beschuldigten über herkömmliche Telekommunikationswege lediglich zu Gesprächen über „Skype“ und damit in verschlüsselter Form verabredeten. Auf Antrag der Staatsanwaltschaft Landshut erließ das Amtsgericht Landshut daraufhin am 2. April 2009 einen Beschluss nach §§ 100 a, 100 b StPO, in dem ausdrücklich auch die Überwachung des verschlüsselten Telekommunikationsverkehrs über HTTPS und über Messenger wie z. B. „Skype“ angeordnet wurde. Mit dem Vollzug dieses Beschlusses beauftragte die Staatsanwaltschaft Landshut das Bayerische Landeskriminalamt.

Mit Schriftsatz vom 2. März 2010 beantragte der Verteidiger eines der Beschuldigten, gemäß § 101 Abs. 7 S. 2 StPO die Rechtswidrigkeit der Maßnahme festzustellen. Das Amtsgericht Landshut wies mit Beschluss vom 4. Oktober 2010 den Antrag zurück und erklärte die Maßnahmen – auch bezüglich der Art und Weise ihrer Durchführung – für rechtmäßig.

Hiergegen erhob der Verteidiger mit Schriftsatz vom 11. Oktober 2010 sofortige Beschwerde. In dem hierzu ergangenen Beschluss vom 20. Januar 2011 stellte das Landgericht Landshut fest, dass der Vollzug des Beschlusses des Amtsgerichts Landshut vom 2. April 2009 rechtswidrig war, soweit grafische Bildschirminhalte (Screenshots) kopiert und gespeichert wurden. Im Übrigen wurde die sofortige Beschwerde des Beschuldigten als unbegründet verworfen.

In den Entscheidungsgründen führte das Landgericht u. a. aus, dass die sogenannte Quellen-Telekommunikationsüberwachung einschließlich der hierfür erforderlichen technischen Maßnahmen zulässig sei. Denn § 100 a StPO erfasse grundsätzlich die Überwachung und Aufzeichnung alle vom Beschuldigten im Rahmen von Telekommunikationsvorgängen zum Zwecke dieser Kommunikation produzierten und für die Weiterleitung an den Kommunikationspartner vorgesehenen Daten. Die Vorschrift schaffe daher grundsätzlich auch eine „Annexkompetenz“ für den technischen Eingriff in das Computersystem des Versenders mittels eines aufgespielten Computerprogramms. Ferner führte das Landgericht aus, dass das Schreiben einer E-Mail vor deren Versendung

aber noch nicht dem Vorgang der Telekommunikation zuzuordnen sei. Zwar bestehe zu diesem Zeitpunkt bereits eine Internetverbindung, doch finde beim Schreiben der E-Mail kein Datenaustausch mit dem Server statt. Denn anders als beim Aufbau einer Telefonverbindung werde die Verbindung zum Server nach dem Aufruf der E-Mail-Maske nicht weiter genutzt.

Die Anordnung des Amtsgerichts Landshut vom 2. April 2009 wurde also nicht – wie in der Frage anklingt – bewusst „missachtet“, was bereits dadurch erkennbar wird, dass das Amtsgericht selbst in seinem Beschluss vom 4. Oktober 2010 den konkreten Vollzug der Anordnung als rechtmäßig angesehen hat. Vielmehr hat das Landgericht Landshut zu der höchstrichterlich noch nicht geklärten Frage, inwieweit bei einer Quellen-Telekommunikationsüberwachung grafische Bildschirminhalte (Screenshots) kopiert und gespeichert werden dürfen, eine andere Auffassung als das Amtsgericht und die mit dem Vollzug befassten Strafverfolgungsbehörden vertreten.

Im Hinblick auf diese landgerichtliche Entscheidung werden die bayerischen Staatsanwaltschaften darauf hinwirken, dass in künftigen vergleichbaren Fällen die Art und Weise einer zulässigen Quellen-Telekommunikationsüberwachung in gerichtlichen Überwachungsanordnungen noch näher konkretisiert und die rechtliche Problematik damit einer weiteren gerichtlichen Klärung zugeführt wird.

Zu 2.:
Die genannten Beschlüsse wurden von der Staatsanwaltschaft Landshut beantragt und vom Bayerischen Landeskriminalamt vollzogen.

Zu 3.:
Für die technische Umsetzung der Maßnahmen zur Überwachung und Aufzeichnung des Telekommunikationsverkehrs gelten die in der richterlichen bzw. staatsanwaltlichen Anordnung genannten Vorgaben sowie die Regelungen der „Verordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation“ (TKÜV), der Technischen Richtlinie zur TKÜV (TR TKÜV) und des Telekommunikationsgesetzes (TKG). Ergänzende oder darüber hinausgehende allgemeine interne Vorgaben zum Umfang von Telekommunikationsüberwachungsmaßnahmen gibt es nicht.

Zu 4.:
Ziel einer Quellen-Telekommunikationsüberwachung ist es, Telekommunikationsinhalte vor ihrer Verschlüsselung bzw. nach ihrer Entschlüsselung zu erheben. Zum Zwecke der Ausleitung der verschlüsselten Telekommunikation wurde im gegenständlichen Ermittlungsverfahren eine Software verwendet, welche über zwei Überwachungsfunktionen verfügte:

- Überwachung und Ausleitung der verschlüsselten Skype-Kommunikation (Sprache/VoIP) vor der Verschlüsselung bzw. nach der Entschlüsselung.
- Automatisierte Erstellung von Kopien/Abbildungen der aktiven Skype- und Internetbrowser-Applikation zur Überwachung der verschlüsselten, auch über HTTPS geführten Telekommunikation. Auf dem Bildschirm des Zielrechners geöffnete andere Programme/Fenster/Applikationen (z. B. geöffnetes Word-Dokument), die nicht mit dem Kommunikationsvorgang in Zusammenhang stehen, wurden nicht aufgezeichnet.

In den Jahren 2005 bis 2008 gab es keine Fälle im Sinne der Fragestellung. Im Jahr 2009 sind zwei Maßnahmen mit zum einen 29.589 und zum anderen 13.558 Aufnahmen der Bildschirmoberfläche zu verzeichnen.

Im Jahr 2010 gab es ebenfalls zwei Maßnahmen. Bei einer Maßnahme wurden 12.174, bei der anderen, die aktuell noch andauert, 11.745 (Stand: 28.02.2011) Screenshots erstellt.