www.jusletter-it.eu

Rolf-Dieter Kargl

# Handlungskatalog für die Evaluierung der Anti-Terror-Gesetze in Österreich (HEAT) – ein erster Überblick

The dimension of government interferences in our private lives and informational self-determination can only be captured correctly when considering the total of all interventions. The paper is meant to give a first overview of the norms that must be evaluated based on the first work package of the project HEAT. In doing so, the neuralgic points in the legal system are scrutinized and the connection between private companies' obligations to cooperate, e.g. based on the E-Commerce law and the Telecommunications law, and powers of authorities according to the Code of Criminal Procedure and the Federal Security Police Act is presented as well as the meshing of authorities within the individual steps of investigative work. Finally, the article provides an outlook towards future steps to the formation of a «catalogue of measures for the evaluation of anti-terror-laws». (ah)

Category: Articles
Region: Austria
Field of law: Data Protection; Data Security

Citation: Rolf-Dieter Kargl, Handlungskatalog für die Evaluierung der Anti-Terror-Gesetze in Österreich (HEAT) – ein erster Überblick, in: Jusletter IT 24 September 2015

## Inhaltsübersicht



## 1. Projektvorstellung

[Rz 1] Das Projekt HEAT (Handlungskatalog für die Evaluierung der Anti-Terror-Gesetze in Österreich) wird vom Arbeitskreis Vorratsdatenspeicherung Österreich in Kooperation mit der Research Institute AG & Co KG getragen und im Rahmen der «NetIdee» durch die Internet Privatstiftung Austria (IPA) gefördert. Das Konzept gewann außerdem im Rahmen der «Netidee»-Förderung den Sonderpreis in der Kategorie «Internet Privacy». Das Konzept von HEAT basiert auf der dritten Forderung der Bürgerinitiative zeichnemit.at, die als Vorbereitung zur vom AKVorrat organisierten «Sammelanfechtung» der Vorratsdatenspeicherung diente. Die von 106.067 Menschen unterstützte Forderung verlangt eine umfassende Evaluierung aller Anti-Terror Maßnahmen (Gesetze) in Österreich im Sinne einer «Gesamtrechnung» aller Überwachungsbefugnisse. HEAT liefert die ersten Schritte einer solchen Gesamtevaluierung mit der Ausarbeitung des Evaluierungsumfangs, der Methoden sowie der Kriterien und stellt praktisch nach den Erfolgen im Kampf gegen die Vorratsdatenspeicherung die Fortsetzung der Initiative dar. Das Projekt listet alle Überwachungsgesetze Österreichs auf, kombiniert diese mit einer Aufarbeitung der relevanten Judikatur, einer Erhebung der durch Sicherheitsbehörden tatsächlich eingesetzten Technologien sowie einer ersten groben Technikfolgenabschätzung und leitet daraus einen Kriterienkatalog für eine Evaluierung aller Anti-Terror-Gesetze ab. Dieses «Pflichtenheft» soll staatlichen und zivilen Organisationen helfen, überschießende und damit potentiell verfassungswidrige Überwachungsbefugnisse zu identifizieren, damit Debatten über Überwachungsgesetze in Zukunft wesentlich strukturierter und sachlicher stattfinden können. Nach erfolgreicher Aufbereitung der zu evaluierenden Gesetze und der herrschenden Judikatur befindet sich das Projekt in der Endphase, deren Kern eine Auflistung bestehender gesetzlicher Überwachungsbefugnisse umfasst, die (auch) der Terrorbekämpfung dienen sollen.

## 2. Das erste Arbeitspaket – Die Aufbereitung der Gesetze

[Rz 2] In seinem ersten Arbeitspaket befasst sich das Projekt HEAT mit der Erfassung und Auflistung der in weiterer Folge in Prüfung zu ziehenden Gesetze, welche einen Konnex zur Terrorismusbekämpfung in Österreich aufweisen. Neben einer beträchtlichen Anzahl an Gesetzen besitzt das Zusammenspiel zwischen dem Sicherheitspolizeigesetz (SPG) und der Strafprozessordnung (StPO), welches in Kapitel 4 eingehend behandelt wird, beträchtliche Bedeutung. Damit Sicherheitsorgane Zugriff auf Verkehrs- und Stammdaten erhalten, bedarf es einer gesetzlichen Grundlage, welche sich aus der Beziehung zwischen SPG, StPO, Telekommunikationsgesetz (TKG) und E-Commerce-

Gesetz (ECG) ergibt. Diese Beziehung wird in Kapitel 3 behandelt. Dabei verursachen zumeist die §§ 278a und b Strafgesetzbuch (StGB) die Grundlage der Problematik. Man findet aber nicht nur in den klassischen Gesetzen Anknüpfungspunkte an die Terrorbekämpfung, sondern auch in weniger naheliegenden Rechtsmaterien. Beispielsweise wäre das Militärbefugnisgesetz (MBG), das Wirtschaftstreuhandberufsgesetz (WTBG), das Finanzstrafgesetz (FinStrG), das Bankwesengesetz (BWG), oder Internationale Abkommen zu nennen. In der Folge soll die vorliegende Arbeit zeigen, dass die verschiedenen Rechtsgrundlagen in der Praxis in wichtigen und teilweise sehr komplexen Zusammenhängen zueinander stehen. Aus diesem Grund soll die Notwendigkeit einer «Gesamtrechnung» der zu evaluierenden Überwachungsbefugnisse gezeigt werden, in dem möglichst praxisnah mit einem fiktiven (aber aus der Realität entwickelten) Fallbeispiel die Interdependenz der Normen nachvollziehbar gemacht wird.

## 3. Case Study – Tierschützerprozess 2.0

[Rz 3] Erfahrungsgemäß lässt sich die Interdependenz der einzelnen Bestimmungen am besten anhand eines konkreten, im Vergleich zu den realen Begebenheiten leicht modifizierten Sachverhalts erklären, welcher auf dem in Österreich berühmt gewordenen sog. «Tierschützerprozess»[1] basiert. Dabei geht man von dem Sachverhalt aus, dass Person A in Geschäft X geht und dortige Pelzmäntel mit einer Spraydose besprüht (beschädigt). Ein paar Tage später findet das Sicherheitsorgan in einem Forum die Nachricht «Ich gehe in das Geschäft des X und werde die Pelzmäntel besprühen» und eine E-Mail in welcher Person A die Tat einem Bekannten ankündigt. Aufgrund von Indizien erwägt das Sicherheitsorgan, dass es sich bei Person A um ein Mitglied einer terroristischen Vereinigung handle. Hier bestehen zwei denkbare Delikte. Zunächst die Sachbeschädigung gem. § 125 StGB mit einem Strafrahmen von bis zu 6 Monaten und die Mitgliedschaft an einer terroristischen Vereinigung gem. § 278b StGB mit einem Strafrahmen von bis zu 10 Jahren.

### 3.1. Erster Ermittlungsschritt – E-Commerce-Gesetz

[Rz 4] Das Ziel von Ermittlungen ist es, den Urheber von einem bereits bekannten Inhalt auszuforschen. Der erste Schritt besteht aus der Ermittlung der IP-Adresse des Absenders bzw. Verfassers der Nachricht/des Forumeintrags. Die Grundlage dafür bildet § 18 Abs. 2 ECG. Der Betreiber eines «Chat-Forum» ist als «Host-Provider» i.S.d. § 16 ECG anzusehen.[2] Dieser Host-Provider speichert fremde Daten (des Nutzers) und stellt die Infrastruktur für die Kommunikation zur Verfügung. Ein Access-Provider vermittelt, in Abgrenzung zum Host-Provider, nur den Zugang zum Internet. Ein «Chatroom» oder «Chat-Forum» ist als ein «Dienst der Informationsgesellschaft»[3] zu verstehen.[4] Somit kann festgestellt werden, dass ein Host-Provider eines Chat-Forums als eine Informationsgesellschaft anzusehen ist. Diese ist nach § 18 Abs. 2 ECG verpflichtet, erforderli-

1 Hierbei handelt es sich um einen Strafprozess gegen mehrere Tierschutzaktivisten. Ermittelt und angeklagt wurde auf Grund des Verdachts, sie hätten eine kriminelle Organisation nach § 278a StGB gebildet und im Zuge derer weitere Straftaten ausgeführt. Siehe auch Mackinger/Pack, §278a: Gemeint sind wir alle! Der Prozess gegen die Tierbefreiungs-Bewegung und seine Hintergründe (2011).

2 VwGH 27. Mai 2009, 2007/05/0280.

3 § 1 Abs. 1 Z 2 Notifikationsgesetz 1999.

4 VwGH 27. Mai 2009, 2007/05/0280.

che Informationen zur Verhütung, Ermittlung, Aufklärung oder Verfolgung gerichtlich strafbarer Handlungen herauszugeben.

## 3.2. Zweiter Ermittlungsschritt – Telekommunikationsgesetz

[Rz 5] In einem zweiten Ermittlungsschritt wird der Subscriber einer Internet-Verbindung zu einer bestimmten IP-Adresse ermittelt. § 99 Abs. 1 TKG regelt die Lösch- bzw. Anonymisierungspflicht der Anbieter. § 99 Abs. 5 TKG regelt die Zulässigkeit der weiteren Verwendung. Schon bei den ersten beiden Ermittlungsschritten wird sichtbar, welche Bedeutung der Gesamtbetrachtung bei der Evaluierung beigemessen werden muss. Durch das Verweisen auf das SPG und die StPO in § 99 Abs. 5 TKG wird die Wechselbeziehung und das Zusammenspiel der unterschiedlichen Bestimmungen deutlich. Grundlegend kann gesagt werden, dass Abs. 1 eine Lösch- bzw. Anonymisierungspflicht für Verkehrsdaten vorsieht und dass eine weitere Verarbeitung nur auf Grundlage des Abs. 5 i.V.m. SPG oder StPO möglich ist.

# 4. Kooperation zwischen SPG und StPO

[Rz 6] Um in das Verhältnis zwischen SPG und StPO näher eingehen zu können und um damit die Problematik bei den Ermittlungsbefugnissen und Rechtsschutzmöglichkeiten zu beleuchten, muss man zunächst die beiden Rechtsgrundlagen voneinander abgrenzen. Während die StPO zur Aufklärung und Verfolgung begangener Straftaten dient, wird das SPG zur Gefahrenabwehr sowie zur allgemeinen Gefahrenerforschung als rechtliche Grundlage der Ermittlungstätigkeiten herangezogen. Bei einem noch nicht beendeten gefährlichen Angriff und einer gleichzeitigen bereits erfüllten Straftat kann es zu einem parallel bestehenden Anwendungsbereich von SPG und StPO kommen. Es können somit beide Gesetze als Grundlage für Ermittlungsmaßnahmen herangezogen werden. Deutlich sichtbar wird dies auch, wenn Straftaten im Rahmen einer kriminellen- oder terroristischen Organisation ausgeführt wurden und weitere Straftaten drohen. Für den Bereich der drohenden Straftat könnte in der Theorie mittels § 21 SPG das Problem entschärft werden, da den Sicherheitsbehörden die Abwehr allgemeiner Gefahren obliegt und davon ausgegangen werden kann, dass ein Vorrang der Gefahrenabwehr und des SPG besteht. Sobald jedoch «*ein bestimmter Mensch der strafbaren Handlung verdächtig ist, gelten ausschließlich die Bestimmungen der StPO*»[5]. Hierdurch wird deutlich, dass für die begangene Straftat die StPO zur Anwendung gelangt, während für die drohende Straftat das SPG Grundlage der Ermittlungstätigkeiten ist. Im Ergebnis kann dies zu einer parallelen Anwendung beider Rechtsgrundlagen führen. Diese Problematik wird in Kapitel 4.2 durch das «Pick & Choose Principle» genauer erklärt.

## 4.1. Ermittlungsbefugnisse im Rahmen von Stammdaten[6]

[Rz 7] Die Sicherheitsbehörden werden durch § 53 Abs. 3a Z 1 SPG ermächtigt, von Betreibern öffentlicher Telekommunikationsdienste (§ 92 Abs. 3 Z 1 TKG 2003) und sonstigen Diensteanbie-

[5] § 22 Abs. 3 SPG. Siehe auch Keplinger, SPG und/oder StPO, Öffentliche Sicherheit 9-10/06, 146.

[6] § 92 Abs. 3 Z 3 TKG.

tern (§ 3 Z 2 ECG) Auskünfte über Namen, Anschrift und Teilnehmernummer eines bestimmten Anschlusses zu verlangen, wenn dies zur Erfüllung ihrer Aufgaben erforderlich ist. Diensteanbieter hinsichtlich eines Chatrooms werden von § 3 Z 2 ECG erfasst.[7] Während bei der Ermittlung nach dem SPG keine erweiterten Voraussetzungen[8] benötigt werden, verlangt § 76a Abs. 2 StPO die Anordnung der Staatsanwaltschaft[9], um die Stammdaten der Nutzer, welche von den Diensteanbietern gespeichert werden, heraus verlangen zu können. Gegen diese Anordnung kann im Stadium des Ermittlungsverfahrens gemäß § 106 Abs. 1 Z 2 StPO Einspruch wegen Rechtsverletzung erhoben werden, worüber nach § 107 StPO ein sachlich und örtlich zuständiges Gericht zu entscheiden hat.

## 4.2. Ermittlungsbefugnisse im Rahmen von Verkehrsdaten[10]

[Rz 8] **§ 53 Abs. 3a Z 2 SPG** berechtigt die Sicherheitsbehörden Auskünfte «*über die Internetprotokolladresse zu einer bestimmten Nachricht und den Zeitpunkt ihrer Übermittlung, wenn sie diese Daten als wesentliche Voraussetzung zur Abwehr einer entweder konkreten Gefahr für das Leben, die Gesundheit oder die Freiheit eines Menschen im Rahmen der ersten allgemeinen Hilfeleistungspflicht, oder eines gefährlichen Angriffs*[11] *oder einer kriminellen Verbindung*[12] *benötigen, zu verlangen.*» Ebenfalls umfasst sind Daten darüber, «*wann und mit welcher IP-Adresse mit welchem Nicknamen auf einem Chatserver kommunizierte wurde*».[13] Im Rahmen der StPO werden Auskünfte über Daten einer Nachrichtenübermittlung wie folgt geregelt.

[Rz 9] **§ 135 Abs. 2 StPO** enthält mehrere Optionen, wie es zu einer gesetzmäßigen Auskunft kommen kann. Dabei werden im Rahmen dieses Papers die zwei bedeutendsten Optionen für die hypothetische (aber nahe an die Realität angelehnte) Fallstudie näher erläutert. Bei Z 2 des § 135 Abs. 2 StPO bedarf es der ausdrücklichen Zustimmung zur Auskunft durch den Inhaber der technischen Einrichtung, die Ursprung oder Ziel einer Übertragung von Nachrichten war oder sein wird. Diese wird für die Herausgabe der Daten für die Aufklärung einer vorsätzlich begangenen Straftat, die mit einer Freiheitsstrafe von mehr als sechs Monaten bedroht ist benötigt. Es ist dies jedoch nur erlaubt, wenn zu erwarten ist, dass dadurch die Aufklärung gefördert wird. Handelt es sich um eine vorsätzlich begangene Straftat mit einer Freiheitsstrafe von mehr als einem Jahr, und kann dadurch die Aufklärung gefördert werden, so ist, wenn auf Grund bestimmter Tatsachen anzunehmen ist, dass dadurch Daten des Beschuldigten ermittelt werden können, die Herausgabe der Daten **ohne** die ausdrückliche Zustimmung des Inhabers der technischen Einrichtung, die Ursprung oder Ziel einer Übertragung von Nachrichten war oder sein wird, gem. § 135 Abs. 2 Z 3 StPO möglich. Grundsätzlich ist festzuhalten, dass kein dringender Tatverdacht erforderlich ist, sondern ein

7 VwGH 24. April 2013, 2011/17/0293.

8 Zu denken wäre hier an eine staatsanwaltschaftliche Anordnung oder eine gerichtliche Bewilligung.

9 § 102 StPO.

10 § 92 Abs. 3 Z 4 TKG.

11 § 16 Abs. 1 Z 1 SPG. Es kann festgehalten werden, dass das Besprühen von fremden Pelzmänteln in einem Geschäft den Tatbestand des § 125 StGB erfüllt und die Ankündigung dieser Tat einen gefährlichen Angriff gem. § 16 Abs. 1 Z 1 darstellt. Das potentiell beeinträchtigte Rechtsgut stellen die Pelzmäntel dar.

12 § 16 Abs. 1 Z 2 SPG. Eine kriminelle Verbindung ist i.S.d. SPG eine Personengruppe von drei oder mehr Menschen, die sich verbinden um fortgesetzt gerichtlich strafbare Handlungen zu begehen.

13 VfGH 29. Juni 2012, B 1031/11-20.

einfacher Tatverdacht genügt[14] und dass jede Ermittlungsart verhältnismäßig i.S.d. § 5 StPO sein muss. Gem. § 137 Abs. 1 StPO sind die Ermittlungsmaßnahmen von der Staatsanwaltschaft auf Grund einer gerichtlichen Bewilligung anzuordnen.

[Rz 10] Der Unterschied zwischen dem SPG und der StPO liegt im Rahmen von Verkehrsdaten also darin, dass bei einer Heranziehung des SPG als Ermittlungsgrundlage es keiner staatsanwaltschaftlichen Anordnung und keiner gerichtlichen Bewilligung bedarf. Daraus entsteht folglich das rechtsstaatlich Risiko, dass es zu einem «Pick & Choose Principle» kommt. Je nachdem welche Gesetzesgrundlage man wählt, werden unterschiedliche Voraussetzungen an die Herausgabe von Verkehrsdaten geknüpft. Es gelten unterschiedliche Rechtsschutzlevel und im Falle einer (angeblichen) anhaltenden Drohung einer Gefahr kann die für die Sicherheitsbehörde «bessere» gesetzliche Grundlage, gewählt werden. «Besser» ist eine Rechtsgrundlage in der Praxis dann, wenn sie weniger Aufwand erfordert, z.B. weil eine Ermittlungsmaßname nicht auf eine schriftliche Genehmigung oder Anordnung einer anderen Stelle warten muss.

## 4.3. Automationsunterstützter Datenabgleich gem § 141 StPO

[Rz 11] Zunächst muss einmal geklärt werden worum es sich bei dem Datenabgleich i.S.d. § 141 StPO handelt. Demnach «*ist ‹Datenabgleich› der automationsunterstützte Vergleich von Daten (§ 4 Z 1 DSG 2000) einer Datenanwendung, die bestimmte, den mutmaßlichen Täter kennzeichnende oder ausschließende Merkmale enthalten, mit Daten einer anderen Datenanwendung, die solche Merkmale enthalten, um Personen festzustellen, die auf Grund dieser Merkmale als Verdächtige in Betracht kommen.*»[15] Dabei werden entweder positive- oder negative Abgrenzungskriterien in den Datenabgleich einbezogen. Je nachdem wird dieser dann positiver- oder negativer Datenabgleich genannt. Beispielsweise, ist der Auszuforschende «Blond» und wird in den Datenabgleich «Brünett» eingegeben, spricht man von einem negativen Abgrenzungsmerkmal. Es werden somit alle Brünetten negativ abgegrenzt. Der Datenabgleich ist nur zulässig, wenn die Aufklärung eines Verbrechens wesentlich erschwert wäre[16], oder wenn es sich um ein Verbrechen nach § 278a oder § 278b StGB handelt.[17]

[Rz 12] Somit kann festgehalten werden, dass in dem fingierten Fall ein Datenabgleich für das Delikt der Sachbeschädigung keine erlaubte Ermittlungsmethode darstellt, da der Strafrahmen im Falle des § 125 StGB bei maximal 6 Monaten liegt und § 141 StPO entweder ein Verbrechen i.S.d. § 17 Abs. 1 StGB[18] oder ein Verbrechen nach § 278a oder § 278b StGB verlangt. Die Problematik hierin besteht, dass diese Ermittlungsmethode bei gegebenen Indizien[19] zur Ermittlung von anderen, geringfügigeren Delikten verwendet werden könnte. Sollte nämlich das Sicherheitsorgan annehmen, dass die Tat im Rahmen einer kriminellen Vereinigung oder einer terroristischen Organisation

14 Vgl. die Unterscheidung z.B. bei Eingriffen in die Persönliche Freiheit: Während allein die Festnahme mit Freiheitsentziehung für max. 96 Stunden gemäß § 171 StPO einen einfachen Tatverdacht genügen lässt, erfordert der zeitlich viel intensivere Grundrechtseingriff der Untersuchungshaft, nach § 173 StPO einen «dringenden Tatverdacht».

15 § 141 Abs. 1 StPO.

16 § 141 Abs. 2 StPO.

17 § 141 Abs. 3 StPO.

18 § 17 Abs. 1 StGB bezeichnet als Verbrechen Delikte mit einem Strafrahmen von mehr als 3 Jahren.

19 Selbst wenn die Indizien im Nachhinein sich als nicht gegeben heraus stellen, so dürfen die Ergebnisse verwertet werden, da sie keinem Verwertungsverbot unterliegen und es zu einer ex ante Prüfung kommt.

begangen wurde, dann können die Daten einer Person in einem Datenabgleich abgeglichen werden, obwohl es bei der Verwirklichung des Grunddelikts (§ 125 StGB) nicht rechtmäßig wäre.

## 5. Conclusio und Ausblick

[Rz 13] Zusammenfassend sei gesagt, dass das Ausmaß der staatlichen Eingriffe in unsere Privatsphäre und in die informationelle Selbstbestimmung sich nur durch die Betrachtung der Summe aller Eingriffe richtig erfassen lässt. Aus diesem Grund kommt es bei der Prüfung und den Effekten bei den gesetzlichen Grundlagen der Ermittlungsbefugnisse darauf an, in wie weit die diversen Bestimmungen in Beziehung zu einander stehen, um die Problematik der Ermittlungsbefugnisse bei terroristischer- oder organisierter Kriminalität zu lösen. Wie die Fallstudie gezeigt hat, bestehen bei dem SPG und der StPO Abgrenzungsprobleme, welche bei genauerer Betrachtungsweise den Schluss zulassen, dass diese für Ermittlungsmaßnahmen gegen die Rechtsschutzinteressen der Betroffenen genützt werden könnten. Als erstes Beispiel seien die unterschiedlichen Rechtschutzmöglichkeiten bei SPG und StPO zu nennen. Hierbei kann es zu einem «Pick & Choose Principle» kommen, wo die gesetzlichen Grundlagen für die Ermittlungsbefugnisse je nach Bedarf gewählt werden können. Desweiteren dürfen bei einer Verbindung zu einer kriminellen- oder terroristischen Organisation Daten auch in den automationsunterstützten Datenabgleich einbezogen werden, die sonst bei einer Tatbestandsverwirklichung bei Delikten mit geringerer Strafdrohung wie z.B. einer Sachbeschädigung nach § 125 StGB nicht rechtmäßig verarbeitet werden könnten. Die hier dargestellten Zusammenhänge sind sozusagen nur die «Spitze des Eisbergs» und sollen lediglich illustrieren, dass die Problematik komplex ist und daher auch in der vollen Komplexität einer Evaluierung zugänglich gemacht werden soll.

[Rz 14] Im aktuellen Stadium des Projekts HEAT kommt es zu einer Zusammenführung aller interdisziplinären Teile aus Technologie, Recht und Sozialwissenschaften. Darauf aufbauend werden die Kriterien zur Evaluierung der Anti-Terror-Gesetze erarbeitet. Dabei wird auch die Judikatur des OGH im «Funkzellen-Urteil»[20] einen wesentlichen Beitrag zur Erarbeitung der Kriterien leisten. Beispielhaft stellte der OGH fest, «dass es sich bei der Funkzellenauswertung um eine äußerst eingriffsintensive und extrem hohe Kosten verursachende Überwachungsmaßnahme handle». Diese Feststellungen schaffen das Fundament für die Kriterien «Intensität der Überwachungsmaßnahme» und «Kosten der Überwachungsmaßnahme». Aktuelle legistische Vorhaben im Bereich der Sicherheit zeigen, dass insbesondere angesichts der komplexen Zusammenhänge, eine Evaluierung offenbar beim Gesetzgeber nicht verankert ist. Das Fehlen einer Evaluierung bedeutet, dass der Gesetzgeber bei der Schaffung von Normen, die Grundrechtseingriffe zulassen, weitgehend einer Rechtfertigung schuldig bleibt. Das Konzept der Europäischen Menschenrechtskonvention und darauf basierend der Europäischen Grundrechtecharta verpflichtet den Staat zur Rechtfertigung bei Grundrechtseingriffen und nicht den einzelnen Bürger. Die Formel wer nichts zu verbergen hat, hat auch nichts zu befürchten verkehrt dieses Paradigma ins Gegenteil.

---

Rolf-Dieter Kargl, Wissenschaftlicher Mitarbeiter, LL.M, Research Institute AG & Co KG –

[20] OGH 5. März 2015, 12 Os 93/14i. Im Wesentlichen behandelt der OGH in jenem Urteil die Verhältnismäßigkeit einer Funkzellenabfrage für einen bestimmten (kurzen) Zeitraum zu später Stunde. Im Ergebnis kam der OGH zu dem Ergebnis, dass es sich um eine rechtmäßige Maßnahme in diesem Fall handelte.

Zentrum für digitale Menschenrechte, Amundsenstraße 9, 1170 Wien, AT; rolf-dieter.kargl@researchinstitute.at; http://researchinstitute.at.