

Verwendung von erlangten Daten aus der elektronischen Kommunikation im Strafprozess – das georgische Recht und internationale Standards*

Von Doktorandin *Tamar Gegeshidse*, Iwane-Dschawachischwili-Staatliche-Universität Tbilisi

I. Einführung

Aufgrund des in den letzten Jahrzehnten erzielten technischen Fortschritts hat sich die Kommunikation zwischen Privatpersonen in die virtuelle Welt verlagert. Die Mittel der elektronischen Kommunikation, wie Internet, Smartphones und Wi-Fi-Technologie, sind Teil des Alltags geworden.¹ Durch die Verbesserung der Computer- und Kommunikationstechnologien ist es möglich geworden, in kürzester Zeit von jedem Ort der Welt jede Art von Informationen weiterzugeben, zu verbreiten oder zu empfangen, was die Möglichkeiten der Kommunikationüberwachung durch die Strafverfolgungsbehörden erweitert. Der Schutz der Privatsphäre während der Überwachung ist nicht nur das Problem eines einzelnen Staates, sondern hat zunehmend globalen Charakter bekommen. Die digitale Grenzenlosigkeit im Internet und das schnelle Tempo der technischen Fortentwicklung stellt die internationale Gesellschaft ständig vor neue Herausforderungen und gewinnt international immer mehr an Bedeutung.

Georgien entwickelt sich rasch in Richtung zur europäischen Integration. Auf diesem Wege wurde das Assoziierungsabkommen zwischen der Europäischen Union und Georgien verabschiedet. Laut des Abkommens verpflichtet sich Georgien, ein hohes Maß an Datenschutz gemäß der im Anhang I des Assoziierungsabkommens erwähnten Richtlinien der Europäischen Union, Übereinkommen des Europarats und anderen internationalen Verträgen zu gewährleisten. Von daher ist es wichtig, die georgische Gesetzgebung in dieser Hinsicht an die internationalen Standards der Kommunikationüberwachung anzugleichen.

* Deutsche Übersetzung des Aufsatzes vom Lektoratsmitglied der DGStZ Herrn *Davit Chikhladze*.

¹ “The right to privacy in the digital age”, Report of the Office of the United Nations High Commissioner for Human Rights, 2014, 3, abrufbar unter: http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf (zuletzt abgerufen am 20.04.2017).

Im vorliegenden Artikel werden international anerkannte Standards der geheimen Überwachung der elektronischen Kommunikation, die Problembereiche des georgischen Rechts und der daraus resultierende Reformbedarf beleuchtet.

II. Die rechtlichen Neuerungen in der georgischen Gesetzgebung hinsichtlich der elektronischen Kommunikationsüberwachung

Das Recht auf Privatleben ist in Georgien ein verfassungsrechtlich verankertes fundamentales Prinzip. Die georgische Verfassung schützt die Unantastbarkeit der Privatsphäre eines Menschen, den Arbeitsplatz, seine persönlichen Notizen, seinen Briefwechsel, seine Telefongespräche oder Äußerungen mittels eines anderen technischen Mediums sowie die durch technische Medien erhaltenen Mitteilungen. Die Einschränkung der oben genannten Rechte ist aufgrund einer Gerichtsentscheidung oder in den gesetzlich vorgesehenen dringenden Notfällen zulässig.

Das Thema hat in Georgien aufgrund des Gesetzes über die operativen Ermittlungsmaßnahmen besonders an Aktualität gewonnen. Das Gesetz regelte das Prozedere der Überwachungsmaßnahmen bis zum August 2014 und war durch ein niedriges Schutzniveau bezüglich der Menschenrechte gekennzeichnet. Wegen seiner Kollision mit den international anerkannten Standards führte dies immer wieder zu Schwierigkeiten. Deshalb hat das georgische Parlament am 1. August 2014 ein neues Gesetzespaket über die geheimen Ermittlungsmaßnahmen verabschiedet, das die diesbezügliche Gesetzgebung grundlegend reformiert und mehr Garantien für die Menschenrechte aufgenommen hat. Aufgrund dieser Gesetzesänderungen sind in der georgischen Strafprozessordnung² eine Vielzahl an rechtlichen Neuerungen entstan-

² Im Folgenden als StPO abgekürzt.

den. Ein neues Kapitel wurde in die StPO eingefügt; in diesem sind folgende Maßnahmen der Datenerlangung aus der elektronischen Kommunikation aufgelistet:

- heimliches Belauschen und Aufzeichnung eines Telefonats;
- Entfernen und Fixation von Informationen aus den Kommunikationskanälen (Kommunikationsmitteln, Rechnernetz, Kabelkommunikation und durch Anschluss an stationäre Anlagen) sowie aus Computersystemen (unmittelbar sowie distanziert) mit dem Ziel, im Computersystem entsprechende Software zu installieren.

Infolge der Gesetzesänderungen ist die geheime Überwachung von Telefongesprächen und Internetaktivitäten nur im Rahmen einer Ermittlungsmaßnahme erlaubt, also nur nach der Einleitung eines Ermittlungsverfahrens und bei begründetem Verdacht auf eine schwere Straftat. Es wurde ein gesetzlicher Katalog der Straftaten erarbeitet, bei denen die geheimen Überwachungsmaßnahmen durchgeführt werden dürfen. Die Kategorien dieser Straftaten wurden dabei eingegrenzt. Die Gesetzgebung hat überdies den Personenkreis eingeschränkt, gegen den die erwähnten Maßnahmen gerichtet sind. Bei den geheimen Ermittlungsmaßnahmen wird auf den Verhältnismäßigkeits- und Notwendigkeitsgrundsatz hingewiesen. Dies bedeutet, dass eine geheime Ermittlungsmaßnahme nur dann erlaubt ist, wenn sie ein legitimes Ziel verfolgt, das im Einklang mit der demokratischen Gesellschaftsordnung steht. Dabei sollte sie angemessen und erforderlich für seine Zweckbestimmung sein und nur dann eingesetzt werden, wenn die Ermittlung über keine anderen Alternativen verfügt, zuverlässige Beweise zu sichern oder dies einen zu hohen Aufwand erfordert. Zudem sollte bei den geheimen Ermittlungsmaßnahmen das Minimierungsgebot beachtet werden. So bedeutet dies etwa, dass die Überwachung derjenigen Personen maximal eingeschränkt werden sollte, deren Telefongespräche für das Verfahren irrelevant sind. Die Frist der Maßnahme wurde streng festgelegt. Die anfängliche Dauer beträgt einen Monat, die maximal zwei Mal verlängert werden darf. Außerdem wurde das Prozedere für die Durchführung der Maßnahme sowie die Vernichtung der erlangten Daten und deren Speicherung ausführlich beschrieben. Eine Neuerung ist auch die rechtliche Regulierung der Benachrichtigungspflicht der Adressaten in der Strafprozessordnung über die Überwachung nach der Ermittlungsmaßnahme.

III. Die Problembereiche der georgischen Gesetzgebung

1. Die Möglichkeit eines direkten Zugriffs zu den Kommunikationskanälen durch die zuständige Behörde

Die Aktualität der geheimen Ermittlungsmaßnahmen wurde durch die Entscheidung des Verfassungsgerichts Georgiens vom 14.04.2016 weiter verschärft, in der die grundlegenden Normen der geheimen Ermittlungsmaßnahmen für verfassungswidrig erklärt wurden. Insbesondere entschied das Verfassungsgericht, dass die Vorschriften des Gesetzes über die elektronische Kommunikation gegen die Verfassung verstoßen haben – die Normen, die die für die geheimen Ermittlungsmaßnahmen zuständigen Behörden berechtigten, die Informationen aus den Kommunikationskanälen in Echtzeit zu erlangen und mit diesem Ziel ein *Lawful Interception Management System*, die für seinen Betrieb erforderliche Ausrüstung und andere geeignete Softwareprodukte im Kommunikationsverkehr einzusetzen.³

Die Verfassungswidrigkeit der Normen war dadurch bedingt, dass für einen direkten Zugriff zu den Kommunikationskanälen eine „professionell interessierte Behörde“, d. h. ein staatlicher Sicherheitsdienst, beauftragt war, die zugleich die Verantwortung für eine erfolgreiche Ermittlung trug.⁴ Nach Auffassung des Verfassungsgerichts war „das Risiko zum unbegründeten Eingriff in die Grundrechte aufgrund der Ermittlungsinteressen hoch“.

Das Problem des direkten Zugriffs zu den Kommunikationskanälen durch die Strafverfolgungsbehör-

³ Verfassungsgericht Georgiens vom 16.04.2016, N1/1/625, 640, 73, 74, abrufbar unter: <http://constcourt.ge/ge/legal-acts/judgments/saqartvelos-saxalxo-damcveli-saqartvelos-moqalaqeebi-giorgi-burdjanadze-lika-sadjaia-giorgi-gociridzetatia-qinqladze-giorgi-chitidze-lasha-tugushi-zviad-qoridze-aaip-fondi-gia-sazogadoeba-saqartvelo-aaip-saertashorisogamchvirvaloba-saqartvelo-aaip-saqar.page> (zuletzt abgerufen am 15.04.2017).

⁴ Verfassungsgericht Georgiens vom 16.04.2016, N1/1/625, 640, 63, abrufbar unter: <http://constcourt.ge/ge/legal-acts/judgments/saqartvelos-saxalxo-damcveli-saqartvelos-moqalaqeebi-giorgi-burdjanadze-lika-sadjaia-giorgi-gociridzetatia-qinqladze-giorgi-chitidze-lasha-tugushi-zviad-qoridze-aaip-fondi-gia-sazogadoeba-saqartvelo-aaip-saertashorisogamchvirvaloba-saqartvelo-aaip-saqar.page> (zuletzt abgerufen am 15.04.2017).

de wurde schon im Fall Zakharov gegen Russland vor dem Europäischen Gerichtshof für Menschenrechte verhandelt. Der Gerichtshof war der Auffassung, dass „das System, das den Sicherheitsdiensten und der Polizei die Möglichkeit gibt, ohne eine Genehmigung des Kommunikationsdienstleisters oder ohne vorherige gerichtliche Genehmigung die Kommunikation jedes einzelnen Staatsbürgers direkt abzufangen, besonders anfällig für den Rechtsmissbrauch ist. Die Notwendigkeit von Schutzmaßnahmen gegen Willkür und Missbrauch scheint besonders groß zu sein. Der Gerichtshof wird daher prüfen, ob die Überwachungsregelungen in der Lage sind, sicherzustellen, dass alle Überwachungsaktionen auf Grund einer ordnungsgemäßen gerichtlichen Genehmigung rechtmäßig durchgeführt werden.“⁵

Unter dem geltenden System betonte das Verfassungsgericht die Erforderlichkeit einer „überzeugenden Prozesstransparenz und von Kontrollmechanismen“ auf der legislativen Ebene.⁶ Die Kontrolle der geheimen elektronischen Überwachungsmaßnahmen ist zugleich international ein umstrittenes Thema. Die Schutzgarantien gegen den Rechtsmissbrauch ohne eine unabhängige Behörde gelten nach internationalen Standards auch als ineffektiv. Obwohl solche Schutzgarantien meist in einer Vielzahl von Regeln ausgedrückt werden, gilt die Einbeziehung aller Zweige der Regierung einschließlich einer unabhängigen Behörde im Überwachungsprozess als grundlegende Schutzgarantie für die Grundrechte.⁷

Das Verfassungsgericht Georgiens hat die Kontrollmechanismen sowohl für die Telefonüberwachung als auch für die Überwachung von Internet-Aktivitäten

als ineffektiv bezeichnet. In Bezug auf die Telefonüberwachung war das Gericht mit der Tatsache unzufrieden, dass das geltende Recht ohne Beteiligung des Inspektors Telefonüberwachung ermöglichte, da die Gesetzgebung die Sicherheitsdienste ermächtigt hatte, solche technischen Möglichkeiten anzuwenden, deren Kontrolle dem Inspektor nicht möglich war⁸. Was die Überwachung von Internetaktivitäten betrifft, vertritt das Verfassungsgericht die Auffassung, dass das Abfangen der Informationen in Echtzeit im Internet tatsächlich seitens des Gesetzgebers mit keinen Kontrollmechanismen verbunden war, außer einer Kontrollmöglichkeit durch den Datenschutzinspektor, die als nicht effektiv erklärt wurde.

2. Vorratsdatenspeicherung

Die Entscheidung des Verfassungsgerichts Georgiens hat auch andere Problempunkte hervorgehoben, wie die Speicherung von personenbezogenen Daten, z. B. sogenannten Metadaten. Dies sind Daten, die Informationen über Kommunikationsquelle, Datum, Art und Dauer der Kommunikation des Benutzers, dessen Standort, die Identität und Telefonnummer und die Internet-Protokoll(IP)-Adresse enthalten. Infolge der Datenanalyse ist es möglich, die Identität einer Person, mit der der Benutzer kommunizierte, sowie die Dauer, den Standort und die Frequenz der Kommunikation während eines bestimmten Zeitraums zu ermitteln.⁹ Von daher kann aufgrund einer Gesamtbewertung dieser Informationen ein detailliertes Profil über das Privatleben eines Menschen erfasst werden.¹⁰

⁵ EGMR vom 04.12.2015, N47143/06, Rn. 270 f., abrufbar unter: <http://hudoc.echr.coe.int/eng?i=001-159324> (zuletzt abgerufen am 14.04.2017).

⁶ Verfassungsgericht Georgiens vom 16.04.2016, N1/1/625, 640, 44 f., abrufbar unter: <http://constcourt.ge/ge/legal-acts/judgments/saqartvelos-saxalxo-damcveli-saqartvelos-moqalaqeebi-giorgi-burdjanadze-lika-sadjaia-giorgi-gociridzetatia-qinqladze-giorgi-chitidze-lasha-tugushi-zviad-qoridze-aaip-fondi-gia-sazogadoeba-saqartvelo-aaip-saertashorisogamchvirvaloba-saqartvelo-aaip-saqar.page> (zuletzt abgerufen am 15.04.2017).

⁷ “The right to privacy in the digital age”, Report of the Office of the United Nations High Commissioner for Human Rights, 2014, 12 f., abrufbar unter: http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf (zuletzt abgerufen am 20.04.2017).

⁸ Verfassungsgericht Georgiens vom 16.04.2016, N1/1/625, 640, 49 f., abrufbar unter: <http://constcourt.ge/ge/legal-acts/judgments/saqartvelos-saxalxo-damcveli-saqartvelos-moqalaqeebi-giorgi-burdjanadze-lika-sadjaia-giorgi-gociridzetatia-qinqladze-giorgi-chitidze-lasha-tugushi-zviad-qoridze-aaip-fondi-gia-sazogadoeba-saqartvelo-aaip-saertashorisogamchvirvaloba-saqartvelo-aaip-saqar.page> (zuletzt abgerufen am 15.04.2017).

⁹ EuGH vom 08.04.2014, NC-293/12, C-594/12, Rn. 26, abrufbar unter: <http://curia.europa.eu/juris/document/document.jsf?docid=150642&doclang=EN> (zuletzt abgerufen am 19.04.2017).

¹⁰ EuGH vom 21.12.2016, NC-203/15, C-698/15, Rn. 99, abrufbar unter: <http://curia.europa.eu/juris/document/document.jsf?text=&docid=186492&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=544422> (zuletzt abgerufen am 19.04.2017).

Das georgische Parlament hat die EU-Richtlinie über die Vorratsdatenspeicherung umgesetzt, die durch den Europäischen Gerichtshof am 8. April 2014 aufgehoben wurde. Als Ergebnis der Umsetzung der Richtlinie wurde im nationalen Recht eine zweijährige Frist für die Speicherung der Daten bestimmt. Der Sicherheitsdienst wurde ferner mit dem Recht auf das Kopieren der Daten ausgestattet.

Durch die oben erwähnte Entscheidung hat das Verfassungsgericht die gesetzlichen Bestimmungen als verfassungswidrig erklärt, die den Sicherheitsdiensten das Recht gewährten, personenbezogene Daten zu kopieren und diese für zwei Jahren zu speichern. Die Verfassungswidrigkeit wurde festgestellt, weil der Gesetzgeber dem Sicherheitsdienst als „für die Ermittlung verantwortliche“ und „professionell interessierte Behörde“ einen uneingeschränkten Zugang auf die sensiblen Informationen eröffnete. Darüber hinaus wurde die Datenspeicherung für einen Zeitraum von zwei Jahren bei jeder möglichen Person ohne vorherige Einschränkung als gravierender Eingriff in die Privatsphäre erklärt. Das Gericht wies außerdem darauf hin, dass es für die Datenspeicherung keine effektiven Kontrollmechanismen gibt. Obwohl das Gesetz für die Verwendung der Daten durch die Ermittlungsbehörde eine gerichtliche Genehmigung oder in dringenden Notfall eine Anordnung der Staatsanwaltschaft voraussetzt, ist nach Auffassung des Gerichts bezüglich des Kopierens der Daten und deren Abfangen kein Kontrollmechanismus vorhanden. In diesem Sinne wurde verdeutlicht, dass es technisch möglich ist, beim Kopieren und bei der Speicherung der personenbezogenen Daten eine sogenannte „alternative Bank zu schaffen, von deren Existenz niemand wissen kann und zu der die Datenschutzinspektoren auch keinen Zugang haben.“¹¹

Die Speicherung der personenbezogenen Kommunikationsdaten ist auch ein Problem auf internationaler Ebene. Nach der Rechtspraxis des Europäischen Gerichtshofs muss der nationale Gesetzgeber klare und

präzise Regeln über die Tragweite und die Anwendung einer solchen Maßnahme wie der Vorratsdatenspeicherung vorsehen. Die Vorratsspeicherung der Daten muss objektiven Kriterien genügen, die einen Zusammenhang zwischen den zu speichernden Daten und dem verfolgten Ziel herstellen. Dabei müssen Personenkreise erfasst werden, deren Daten geeignet sind, einen zumindest mittelbaren Zusammenhang mit schweren Straftaten sichtbar zu machen, auf irgendeine Weise zur Bekämpfung schwerer Kriminalität beizutragen oder eine schwerwiegende Gefahr für die öffentliche Sicherheit zu verhindern. Der Gerichtshof ist noch strenger, wenn es um den Zugang zu auf Vorrat gespeicherten Daten geht. Strafverfolgungsbehörden dürfen Zugang grundsätzlich nur zu den Daten von Personen erhalten, die im Verdacht stehen, eine schwere Straftat zu planen, zu begehen oder begangen zu haben oder auf irgendeine Weise in eine solche Straftat verwickelt zu sein.¹²

IV. Die Neuregelung der geheimen Überwachungsmaßnahmen

Das georgische Parlament hat am 22. März 2017 ein neues Paket von Gesetzesänderungen erlassen, um die Vorschriften an die Entscheidung des Verfassungsgerichts anzupassen. Die grundlegende Anforderung des Verfassungsgerichts, eine unabhängige Behörde zu schaffen, die die geheimen Überwachungsmaßnahmen technisch umsetzt und dabei keine Ermittlungsfunktion hat, wurde mit der Schaffung einer operativ-technischen Agentur erfüllt. Sie wurde als öffentlich-rechtliche juristische Person im Sicherheitsdienst gebildet. Wie die geheimen Überwachungsmaßnahmen in der Zukunft technisch eingesetzt werden und inwieweit die neue Agentur den Anforderungen des Verfassungsgerichts genügt, wird sich in der Rechtspraxis zeigen.

Laut der Gesetzesänderungen wurden technische Möglichkeiten der geheimen Überwachungsmaßnahmen, die die Agentur zur Verfügung hat, konkretisiert, was begrüßenswert ist. Um eine Telefonüberwachung durchzuführen und von dem Betreiber der elektroni-

¹¹ Verfassungsgericht Georgiens vom 16.04.2016, N1/1/625, 640, 64 f., abrufbar unter: <http://constcourt.ge/ge/legal-acts/judgments/saqartvelos-saxalxo-damcveli-saqartvelos-moqalaqeebi-giorgi-burdjanadze-lika-sadjaia-giorgi-gociridzeta-tatia-qinqladze-giorgi-chitidze-lasha-tugushi-zviad-qoridze-aaip-fondi-gia-sazogadoeba-saqartvelo-aaip-saertashoriso-gamchvirvaloba-saqartvelo-aaip-saqar.page> (zuletzt abgerufen am 15.04.2017).

¹² EuGH vom 21.12.2016, NC-203/15, C-698/15, Rn. 109-111 und 119, abrufbar unter: <http://curia.europa.eu/juris/document/document.jsf?text=&docid=186492&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=544422> (zuletzt abgerufen am 19.04.2017).

schen Kommunikationsdienste die Daten in Echtzeit zu erlangen, darf die Agentur im Rahmen seiner stationären technischen Möglichkeiten ein *Lawful Interception Management System*, die für seinen Betrieb erforderliche Ausrüstung und andere geeignete Softwareprodukte einsetzen. Ferner ist es ein Novum, dass der Inspektor das Recht hat, statt den Einsatz einer geheimen Überwachungsmaßnahme zu genehmigen, diese in den gesetzlich vorgesehenen Fällen auszusetzen, z. B. wenn dem Inspektor die gerichtliche Genehmigung oder im dringenden Notfall eine Anordnung der Staatsanwaltschaft elektronisch oder in Papierform nicht überreicht wurde.

Insgesamt betreffen die Kontrollmechanismen der geheimen Überwachungsmaßnahmen nach dem georgischen Recht grundsätzlich nur die Anfangsphase der Maßnahmen. Bei dem Einsatz der Maßnahme wird diese von dem Inspektor auf ihre Rechtmäßigkeit geprüft. Besser wäre es jedoch, die ganze Maßnahme während ihres Verlaufs zu kontrollieren, auch durch die Einbeziehung der Gerichte. Die gerichtliche Kontrolle der geheimen Überwachungsmaßnahmen ist in Georgien schwach ausgeprägt und betrifft nur die Anfangsphase der Maßnahme und deren Verlängerung. Obwohl die Gesetzgebung bestimmte Ausnahmen kennt, wie z. B. die gerichtliche Beteiligungspflicht bei der Vernichtung der erlangten Daten, sind die Gerichte aufgrund des im StGB verankerten Wettbewerbsprinzips wenig an dem Gesamtprozess der geheimen Überwachungsmaßnahmen beteiligt, insbesondere während des Verlaufs oder nach dem Abschluss der Maßnahmen. Dies bringt folglich Schwierigkeiten bei der Kontrolle der geheimen Ermittlungsmaßnahmen mit sich.

Die Frist der Vorratsdatenspeicherung wurde nach den Gesetzesänderungen auf 12 Monate verkürzt und kann nur maximal für drei Monate beim Vorliegen der besonderen Voraussetzungen verlängert werden. Was die MetadatenSpeicherung angeht, hat der Europäische Gerichtshof die durch die Richtlinie vorgesehenen Fristen der Datenspeicherung für mindestens sechs Monate und maximal zwei Jahre als nicht verhältnismäßig erklärt. Jedoch hat der Gerichtshof weder in der Entscheidung aus dem Jahr 2014 noch in der aus dem Jahr 2016 eine konkrete Frist festgelegt. Daher kann man nicht eindeutig sagen, was eine verhältnismäßige Datenspeicherung nach internationalen Standards wäre. Wie der Europäische Gerichtshof in diesem Fall besagt, soll die

vorgesehene Dauer der Vorratsspeicherung im nationalen Recht auf das absolut Notwendige beschränkt werden.¹³

Durch das System der Kontrolle der zentralen Datenbank der elektronischen Kommunikation wird der Inspektor in Echtzeit über die Logging-Daten der Zentralbank und Aktivitäten in den personenbezogenen Daten benachrichtigt. Was die theoretische Möglichkeit einer sogenannten „alternativen Datenbank“ und deren Gefahren angeht, ist der Ausschluss solcher Gefahren von der Unabhängigkeit der Behörde abhängig, die die Datenbank kopieren darf, da die Unabhängigkeit der Behörde das theoretische Risiko der Schaffung einer solchen Bank reduziert.

V. Zusammenfassung

Zusammenfassend lässt sich sagen, dass in Georgien das Hauptproblem der direkte Zugang zu den Verbindungskanälen des Staates ist. Diese soll durch die Unabhängigkeit einer Behörde balanciert werden, die die geheimen Überwachungsmaßnahmen technisch umsetzt. Es ist eindeutig, dass die georgische Gesetzgebung in der letzten Zeit einige Fortschritte hinsichtlich der Verbesserung des Menschenrechtsstandards erzielt hat. Jedoch bleibt die Erlangung der Daten aus der elektronischen Kommunikation und deren Verwendung im Strafprozess weiterhin ein aktuelles und schwieriges Problem im Strafprozessrecht. International wird die Verstärkung der Menschenrechtsstandards jedoch aktiv vorangetrieben. So muss Georgien auch mit in Europa laufenden Prozessen mithalten. In diesem Sinne ist die Europäisierung der georgischen Gesetze weiter erforderlich.

¹³ EuGH vom 21.12.2016, NC-203/15, C-698/15, Rn. 108, abrufbar unter: <http://curia.europa.eu/juris/document/document.jsf?text=&docid=186492&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=544422> (zuletzt abgerufen am 19.04.2017).