DFG Graduiertenkolleg
Privatheit und Digitalisierung

UNIVERSITÄT PASSAU

IN DIESER AUSGABE

AUSGABE NR. 12, DEZEMBER 2019

Inhalt

Liebe Leserinnen und Leser,

die Geschenke im Onlinehandel bestellt, Alexa mit einer Playlist an Christmas-Songs ausgestattet, die Weihnachtskorrespondenz per e-card versendet und die Verwandtschaft per Skype unter den Tannenbaum geholt – nicht nur vor und während der Feiertage erleichtern uns digitale Anwendungen aller Art den mitunter stressigen Alltag. Bekanntermaßen hinterlassen wir jedoch bei all diesen Aktivitäten Datenspuren im Netz. Vermeintlich kostenlose Anwendungen werden im digitalen Raum längst mit einer anderen Währung beglichen: mit personenbezogenen Daten. Doch lassen sich diese angesichts umfangreicher Datenerhebungen digitaler Konzerne überhaupt schützen und, wenn ja, wie?

Kürzlich wurde in der Berichterstattung (Tagesschau, SZ) die Verpflichtung von Webmail-Diensten zur Protokollierung und Herausgabe von NutzerInnendaten aufgrund von telekommunikationsrechtlichen Vorschriften erneut aufgegriffen. Dabei kam es zu irreführenden und teilweise unzutreffenden Einschätzungen. Ein E-Mail-Dienst-Anbieter, *Posteo*, nahm sich der Aufgabe an, die rechtliche Sachlage richtigzustellen. Unter anderem diesen E-Mail-Dienst-Anbieter exemplarisch als datensparsame Alternative vorstellend beleuchten **Lea Watzinger** und **Felix Sobala** Alternativen zu gängigen Internet-Anwendungen.

Ergänzend dazu beschäftigt sich **Patrick Herget** vor dem Hintergrund der Entscheidungen des Europäischen Gerichtshofs zu *Gmail* und *SkypeOut* mit der rechtlichen Einordnung internetbasierter Kommunikationsdienste. Die Urteile des EuGH drehen sich um die Frage, wann diese Dienste den bereichsspezifischen Regulierungen des Telekommunikationsrechts unterfallen, wobei die Verantwortlichkeit für die ganz oder überwiegende Signalübertragung zum entscheidenden Kriterium wird.

In Brasilien zogen die Ermittlungen rund um die Operation Lava Jato (»Autowäsche«) den größten Korruptionsskandal in der Geschichte des Landes nach sich und hatten bei den nächsten Wahlen einen politischen Rechtsruck zur Folge. Durch die Veröffentlichung geleakter Telegram-Nachrichten kamen jedoch Zweifel an der Unbefangenheit der an den Untersuchungen beteiligten Beamten auf. Am Beispiel der Bekanntmachung privater Inhalte wägt **Gustavo Gil Gasiola** das Recht auf Privatheit Einzelner gegen das Recht der Öffentlichkeit auf Informationsfreiheit ab.

Alexander Ponomariov befasst sich mit den mapping-Aktivitäten der Russisch-Orthodoxen Kirche. Als Teil einer digitalen Öffentlichkeitsstrategie veröffentlicht diese eine Online-Karte, auf der ihr kanonisches Territorium weltweit verzeichnet ist bzw. als solches deklariert wird. Diese territoriale Verdatung kann als Ausdruck einer Inanspruchnahme gewertet werden.

Neben aktuellen Veranstaltungshinweisen erfahren Sie, welche Publikationen kürzlich im Kontext unseres Kollegs erschienen sind. Zudem wirft **Marcel Schlegel** einen Rückblick auf die Tagung »Verantwortung in digitalen Kulturen«, zu der das Graduiertenkolleg im Frühjahr dieses Jahres eingeladen hatte. In den Steckbriefen können Sie neue Mitglieder unserer Forschungseinrichtung kennenlernen.

Wir wünschen Ihnen viel Spaß bei der Lektüre.

Prof. Dr. Kai von Lewinski
Sprecher des DFG-Graduiertenkollegs 1681/2 »Privatheit und Digitalisierung«

Dr. Jenny Bauer & Dr. Alexander Ponomariov
Postdocs am DFG-Graduiertenkolleg 1681/2 »Privatheit und Digitalisierung«.

Kilian Hauptmann, M.A.
Wissenschaftlicher Koordinator am DFG-Graduiertenkolleg 1681/2 »Privatheit und Digitalisierung«.

Alternative Internetanwendungen und was sie anders machen

Über Geschäftsmodelle, Datenverarbeitungsebenen und gesellschaftliche Aspekte

Foto: Colourbox.de

von Lea Watzinger und Felix Sobala

In times of increasing data collection and online communication as a prerequisite for social participation, many internet users seem to have resigned themselves to the large tech companies — enjoying advantages and coping with risks of data disclosure. However, there are some alternative offers in the market. This contribution presents two European internet applications — *Posteo* (e-mail service) and *Startpage* (search engine). Both have strict privacy policies, featuring the principle of data minimisation. Providing these examples, the authors evolve different aspects that distinguish these applications from common ones (such as GMX, Web.de or Google). Taking into account the current jurisdiction, the article analyses their business models, the different types of data processing according to current telecommunications and telemedia law, as well as their additional benefits for individuals and society.

A. Internetanwendungen

Die Digitalisierung hat Einzug in weite Teile des Lebens gehalten und zu einem technisch-gesellschaftlichen Zustand geführt, den man als »Digitalität«[1] benennen kann. Kennzeichnend für diesen Prozess ist unter anderem eine rapide Zunahme von technisch gestützter Kommunikation. Moderne digitale Kommunikationsmöglichkeiten durch E-Mail-, Messenger- oder (Video-)Telefonie-Dienste – bekannte Vertreter sind beispielsweise *WhatsApp*, *Skype*, *iMessage* oder *Facetime* – erleichtern den Alltag insofern, als dass sie den Austausch mit anderen vereinfachen und flexibilisieren und räumliche Distanzen überwinden helfen; vom heimischen Wohnzimmer oder dem New Yorker Büro aus wird die Teilhabe an Ereignissen und Lebenseindrücken von den entlegensten Orten der Welt Realität. Für Menschen, die aufgrund körperlicher Hindernisse in ihrer Bewegungs- oder Reisefähigkeit eingeschränkt sind, können diese Anwendungen eine große Bereicherung darstellen. Insgesamt handelt es sich um Anwendungen, die kaum mehr aus dem Alltag wegzudenken sind: Anwendungen, die man braucht, um am kommunikativen Sozialleben und erst recht am Geschäftsleben partizipieren zu können.

Auch die Bedeutung von Suchmaschinen lässt sich anhand des mittlerweile fest in der deutschen Sprache verankerten Verbs ›googeln‹ erahnen. Wieviel einfacher, schneller und mit welch niedrigeren Zugangsvoraussetzungen lässt sich heutzutage googeln als früher recherchieren. Sicherlich handelt es sich auch dabei um ein Beispiel für eine Internetanwendung, die niemand mehr missen möchte.

In der Kritik stehen jedoch einige unter anderem sehr populäre Anwendungen, weil sie ihre NutzerInnen teils im Unklaren lassen – oder jedenfalls nicht für die durchschnittlichen VerbraucherInnen hinlänglich explizit machen[2] –, welche Daten sie (genau) sammeln und zu welchen Zwecken (genau) diese (tatsächlich) verarbeitet werden. Durch die Lektüre der jeweiligen Datenschutzerklärungen kann – beziehungsweise sollte – zwar eine gewisse Informierung möglich sein;[3] zur Nutzungserfahrung der großen Mehrheit von AnwenderInnen scheint dies jedoch nicht zu gehören. Regelrechte ›Skandale‹ und ›Datenlecks‹ erschüttern die Vertrauensbeziehung zu und Ansehen von nicht nur einigen wenigen Dienstanbietern, sondern unterwerfen in den oberflächlichen öffentlichen und teilweise dystopisch geführten Diskursen häufig die komplette Digitalbranche einem gewissen Generalverdacht.[4]

Manchmal scheint es, als herrsche auf VerbraucherInnenseite nur noch Resignation gegenüber den gefühlt ›übermächtigen‹ Internetkonzernen – man hat sich mit der Situation abgefunden, man profitiert von den Nutzen, und mit den Risiken hat man sich scheinbar arrangiert respektive blendet sie aus.

Wir möchten zwei alternative Internetanwendungen, einen E-Mail-Dienst-Anbieter, *Posteo*, und eine Suchmaschine, *Startpage*, vorstellen, die es anders machen – und vor allem, was es ist, das sie anders machen. Mit drei entscheidenden Aspekten – dem Geschäftsmodell (B.), den zu unterscheidenden Ebenen der Datenverarbeitung (C.) sowie dem, was unsere vorgestellten Alternativen zusätzlich zur Einhaltung des rechtlichen Rahmens auszeichnet (D.) – setzen wir uns dabei auseinander.

I. *Posteo*

Posteo[5] ist ein Unternehmen aus Berlin, wurde 2009 gegründet und möchte als unabhängiger, nicht zu den großen Internetunternehmen gehöriger deutscher Anbieter »einen Impuls für mehr Sicherheit, Datenschutz und Nachhaltigkeit im Internet geben. Und Alternativen anbieten.« Ihre Server stehen in deutschen Rechenzentren in Frankfurt am Main, Bielefeld und Berlin.

II. *Startpage*

Startpage ist eine europäische Suchmaschine mit Unternehmenssitz in den Niederlanden, die sich – wie *Posteo* – dem Datenschutz verschrieben hat.[6] Sie nennt sich »die diskreteste Suchmaschine der Welt«. *Startpage* verwendet die Ergebnisse der Google-Suche, indem sie die Suchanfragen anonymisiert an *Google* sendet und den NutzerInnen dann die Suchergebnisse zurückschickt; *Startpage* ›kauft‹ sozusagen die Suchergebnisse ein.

B. Geschäftsmodelle und Motivationen

Posteo bietet E-Mail-Postfächer zum Preis von einem Euro pro Monat an.[7] *Posteo* verlangt Geld für seine Services; es handelt sich also nicht um ein sogenanntes *Freemium*[8]-Angebot. Im Gegensatz zu anderen, bekannteren Anbietern, die ihre Dienste meist ohne Gegenleistung in Geld zur Verfügung stellen[9] – was allerdings nicht bedeuten muss, dass sie *umsonst* angeboten werden – möchte *Posteo* die Leistungen im Austausch mit einer transparenten Gegenleistung in Geld anbieten und verzichtet dafür auf Praktiken, durch die sich andere Anbieter finanzieren. *Posteo* finanziert sich nicht durch Werbung, sondern ausschließlich durch die Entgelte (in Geld) der NutzerInnen und betreibt

keinen Datenhandel;[10] die Anmeldung und Bezahlung sind sogar anonym möglich.

Startpage hingegen finanziert sich durch nicht personalisierte Werbeanzeigen, die ohne Tracking oder das Anlegen von Profilen eingeblendet werden. Die Suchergebnisse können zur Finanzierung »ein paar klar gekennzeichnete ›gesponserte Links‹ enthalten«.

Zwar könnte man der Ansicht sein, dass personalisierte Werbung gegebenenfalls interessanter ist, wenn Anbieter oder werbende Drittunternehmen die eigenen Interessen besser einschätzen können. Man sollte sich jedoch vergegenwärtigen, dass die Motivationslage eines Anbieters, der Services *lediglich* im Gegenzug zu der Möglichkeit, persönliche Daten zu verarbeiten, anbietet, eine andere ist. Ein Anbieter, dem die NutzerInnen keine andere Möglichkeit der Refinanzierung geben, wird (im Zweifel) bemüht sein, möglichst viel über diese herauszufinden, über sie in Erfahrung zu bringen oder ihr Verhalten zu analysieren, um sich aus diesem Wissen – bestenfalls in Umsetzung in entsprechende Werbung – zu finanzieren. In diesem Zusammenhang mag man der Ansicht sein, dass unabhängig vom möglichem Manipulationspotenzial personalisierte Werbung ›an sich nichts Schlechtes‹, lediglich die dazu notwendig vorgelagerte Datensammlung und Verwaltung in Profilen problematisch ist. Im Falle der Finanzierung durch eine Gegenleistung in Geld jedoch wird ein Anbieter über die intrinsische Motivation einer politischen Agenda hinaus bemüht sein, dem Versprechen eines ›hohen Datenschutzstandards‹ nachzukommen; KundInnen würden bei Bekanntwerden etwaigen Enttäuschens dieses Versprechens diesem Dienst sicherlich den Rücken zuwenden – allein aus diesem Grund hat ein ›datenschutzversprechender‹ Anbieter eine extrinsische Motivation, das in ihn gesteckte Vertrauen nicht zu enttäuschen, das Renommee nicht zu ›verspielen‹. Das Vertrauen in viele Internetdienste wurde mehrfach erheblich erschüttert, sodass wir eigentlich damit rechnen müssten, dass ihre Angaben gerade *nicht* wahrheitsgemäß sind. *Posteo* macht es nun zum Geschäftsmodell, auf den Datenschutz abzuzielen und eine neue Vertrauensbeziehung zu den NutzerInnen durch eine betont transparente Geschäftspolitik aufzubauen.[11]

Foto: Colourbox.de / YekoPhotoStudio

C. Ebenen der Datenverarbeitung

I. Vertikale Ebene: Back- und Front-End

Plattform-Dienste wie *Facebook* oder *Instagram* bieten Möglichkeiten, von sich im Internet eingestellte Informationen – wie demographische Angaben, Postings, Bilder oder Videos – nur festgelegten Kreisen von RezipientInnen gegenüber zu öffnen. Diese Einstellungsmöglichkeiten werden häufig mit »Privatsphäreeinstellungen«, »Privatsphärenschutz« oder »Datenschutz« betitelt. Fraglich in diesem Zusammenhang ist jedoch zum einen, wie viele NutzerInnen sich *tatsächlich* ausgiebig mit den Einstellungsvarianten, -konsequenzen und -abwägungen auseinandersetzen. Zum anderen – und das scheint noch deutlich relevanter und oftmals ganz vergessen zu werden – muss das nicht bedeuten, dass, nur weil bestimmte persönliche Informationen nicht anderen durch die Plattform zugänglich gemacht werden oder dargestellt werden, die jeweiligen Plattformbetreiber oder Diensteanbieter diese Informationen nicht im (für die bloß Nutzenden unsichtbaren) Hintergrund der Anwendung (Back-End) ›haben‹ oder nutzen (können), obwohl sie auf der für die Nutzenden einsehbaren Anwendungsoberfläche (Front-End) nicht aufscheinen. Das ist je nach den Datenschutzbestimmungen der jeweiligen Diensteanbieter zu beurteilen. Zudem ist vorauszusetzen – und für die durchschnittlichen NutzerInnen schon gleich gar nicht zu prüfen möglich –, dass die Diensteanbieter auch *tatsächlich* nur die in den jeweiligen Datenschutzerklärungen festgelegten Datenverarbeitungen und nur zu den dort angegebenen Zwecken vornehmen. Hier können allerdings Zertifizierungen und Auditierungen Abhilfe im Hinblick auf die Kontrollierbarkeit für Verbraucher und Verbraucherinnen schaffen. Aufgrund dieses Über-/Unterordnungs-Verhältnisses zwischen Anbietern und Nutzenden bezüglich der Einsicht in die *tatsächlich* stattfindenden Datenverarbeitungsvorgänge kann man in diesem Zusammenhang zur Veranschaulichung von einer ›vertikalen Ebene‹ der Datenverarbeitung sprechen.

Die besprochenen Einstellungen schützen nicht vor der Kenntnisnahme durch die Plattformbetreiber, Diensteanbieter und gegebenenfalls deren Werbepartner oder – und das sollte immer mitgedacht werden – dem Missbrauchspotenzial, was eben dem Vorhandensein eines Datenbestandes immer automatisch innewohnt.[12] Die strikte Handhabung von »Privatsphäreeinstellungen« mag insofern zwar vor der Einsichtnahme durch unbekannte dritte NutzerInnen der Plattformen und einer möglichen Vermischung der persönlichen Lebenskontexte schützen, aber nicht mehr und auch nicht weniger. *Posteo* verringert die vertikale Wissensdiskrepanz durch Veröffentlichung ihrer Transparenzberichte sowie eines ihnen geltenden Prüfberichts der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, *Startpage* kann mit zahlreichen Auszeichnungen aufwarten, die das Übereinstimmen ihrer Handlungen mit ihren Datenschutzversprechen untermauern.

II. Horizontale Ebene: Bestands-, Nutzungs- beziehungsweise Verkehrs- und Inhaltsdaten

Im (telemedien-, telekommunikations- und datenschutz-)rechtlichen Zusammenhang wird zwischen *Bestands-*, *Nutzungs-* beziehungsweise *Verkehrs-* und *Inhaltsdaten* unterschieden.[13] Diese Unterscheidung – zur Veranschaulichung kann man sie als eine Differenzierung auf ›horizontaler Ebene‹ bezeichnen – wollen wir zur Sensibilisierung für unterschiedlichste Datenarten und -verarbeitungsvorgänge kurz erläutern:

Als *Bestandsdaten* werden Daten bezeichnet, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses zwischen dem Anbieter und den NutzerInnen erhoben werden (§ 3 Nr. 3 Telekommunikationsgesetz [TKG] beziehungsweise § 14 Abs. 1 Telemediengesetz [TMG]). Das sind zum Beispiel der Name oder die Anschrift einer Person.

Nutzungsdaten sind solche Daten, die für die Ermöglichung der Inanspruchnahme eines Telemediendienstes beziehungsweise für die Abrechnung notwendig sind (§ 15 Abs. 1 S. 1 TMG); als solche bezeichnet man also Daten, die durch die *Nutzung* eines Dienstes bedingt sind. Dazu zählen insbesondere Merkmale zur Identifikation der Nutzenden, Angaben zu Beginn und Ende sowie des Umfangs der Nutzung sowie Angaben über die in Anspruch genommenen Dienste (§ 15 Abs. 1 S. 2 TMG).

Verkehrsdaten sind solche »Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden« (§ 3 Nr. 30 TKG, siehe zu deren Verarbeitung insbesondere auch § 96 TKG). *Nutzungsdaten* ist somit der Terminus, der im Zusammenhang mit Telemediendiensten, *Verkehrsdaten* der Terminus, der im Zusammenhang mit Telekommunikationsdiensten verwendet wird.[14]

Der Begriff *Inhaltsdaten* ist rechtlich nicht definiert, wird aber zur Beschreibung der Daten verwendet, die *Inhalt* der jeweiligen Dienstenutzung sind.

Daten, die nicht den eigentlichen Anwendungsinhalt (beziehungsweise im Kommunikationskontext nicht den eigentlichen Kommunikationsinhalt[15]) betreffen, sondern Informationen zu den Umständen der Anwendungsnutzung (beziehungsweise der jeweiligen Kommunikation) beinhalten, werden auch als ›Metadaten‹ bezeichnet. Allgemeiner gesprochen versteht man unter Metadaten respektive unter Metainformationen: »technische und/oder organisatorische Details zu anderen Informationen. Es handelt sich also nicht um den eigentlichen Inhalt, sondern um Zusatzinformationen.«[16] Dabei *kann* es sich um *Bestands-*, *Nutzungs-* oder *Verkehrsdaten* handeln, es kann sich jedoch auch um *davon verschiedene* Daten handeln. Wann etwas das *eigentliche* Datum – den eigentlichen Inhalt – und wann etwas ein dazu gehöriges *Metadatum* darstellt, kommt immer auf den durch den jeweiligen Einzelfall bedingten Kontext und Blickwinkel an. Daher lässt sich keine generelle Aussage darüber treffen, bei welchen Daten es sich um Metadaten handelt: *Bestands-*, *Nutzungs-* und *Verkehrsdaten* und Metadaten stehen folglich nicht in einem Teilmengenverhältnis – in dem Sinne, dass sich die einen aus den anderen zusammensetzen –, sondern im Sinne eines Schnittmengenverhältnisses – insofern, als dass es zu Überschneidungen kommen kann.

In alltäglichen Datenschutzdiskussionen wird mit Aussagen wie »Ich gebe da keine persönlichen Sachen an« oftmals lediglich auf die Inhaltsebene, allenfalls auch noch auf die Ebene der Bestandsdaten angespielt. Was dabei übersehen wird, ist, dass auch die Metadaten – und oftmals erst recht diese Daten – sehr genaue und erschreckend prägnante Erkenntnisse zulassen. Beispielsweise ermöglichen *bloße* Bewegungsprofile Rückschlüsse auf die Lebensweise, -umstände, den Beruf, Gewohnheiten, Präferenzen und Beziehungen von Nutzenden.[17]

Welche Daten erhebt nun *Posteo*? Was Bestandsdaten betrifft, so geben sie an: »Wir erheben und speichern grundsätzlich keine Bestandsdaten (wie Namen, Adressen, etc.) von Ihnen. Sie geben bei der Registrierung weder Bestandsdaten an, noch werden sonstige personenbezogenen Daten erhoben.«

Was die Erhebung und Erfassung von *Nutzungsdaten*[18] anbelangt, so speichert *Posteo* keine auf KundInnen beziehbaren IP-Adressen:[19] weder im Falle des Besuchs

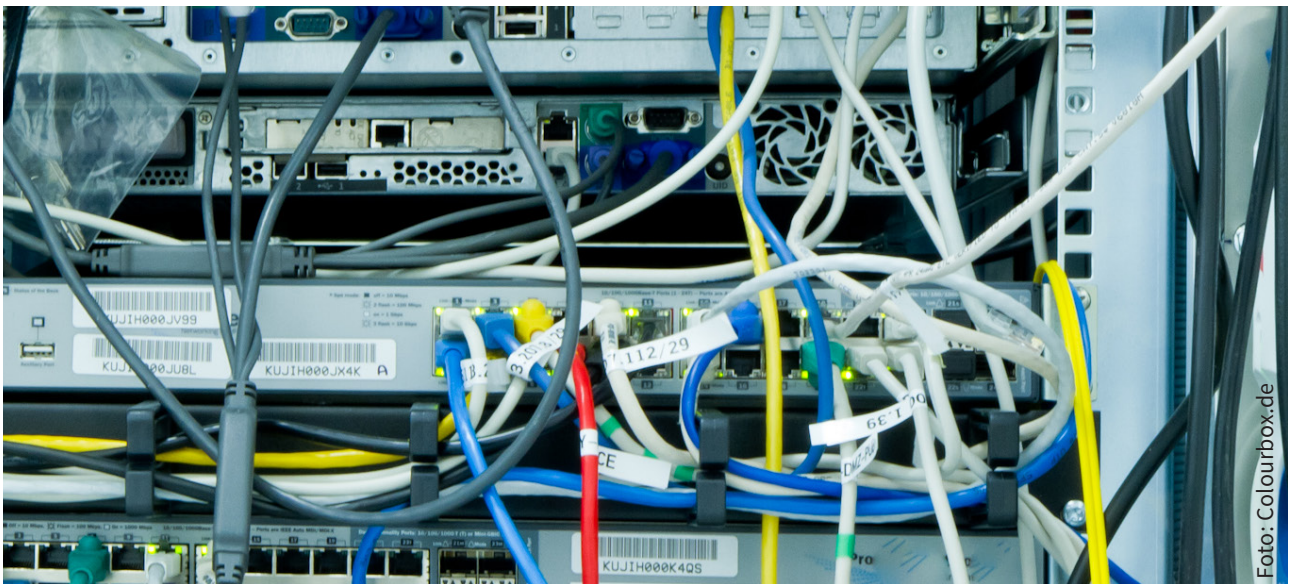
ihrer Website, der Verwendung ihres Kontaktformulares oder des Webmailers, des Abrufes von E-Mails über IMAP oder POP3 noch des Einlieferns von E-Mails über SMTP zum Versand. Lediglich IP-Adressen von E-Mail-Servern anderer Anbieter werden ihnen bei der Kommunikation über SMTP zwischen den E-Mail-Servern bekannt, also beispielsweise von GMX- oder Google-Servern.

Inwiefern *Posteo* die kundenbezogene Erhebung von IP-Adressen zwar (ihrem Geschäftsmodell und anscheinend aufrichtigen Bemühen nach) vermeiden mag,[20] aber faktisch (technisch betrachtet) dennoch Zugriff auf diese haben *könnte* oder sogar *müsste*, um sie Strafverfolgungsbehörden zugänglich zu machen, wurde zu einem Gegenstand, mit dem sich das Bundesverfassungsgericht auseinandergesetzt hat[21]. Im Rahmen eines Ermittlungsverfahrens gegen einen Nutzer kam es zu einer Anordnung der Sicherung und Herausgabe von IP-Adressen an *Posteo*, die im weiteren Verlauf schließlich zu einer Verfassungsbeschwerde vor dem Bundesverfassungsgericht führte. In diesem Verfahren wurden unterschiedliche Ansichten bezüglich der (rechtlichen) Pflicht beziehungsweise der (theoretisch bestehenden, technisch-faktischen) Möglichkeit der Protokollierung und Herausgabe von IP-Adressen der KundInnen vertreten und geäußert.[22] Schlussendlich stellte das Bundesverfassungsgericht fest, *Posteo* mache geltend, man

> »verfüge über die öffentlichen IP-Adressen seiner Kunden nicht. Im gesamten Zugriffsbereich [...] lägen weder intern noch an den Außengrenzen [...] IP-Adressen mit Nutzerbezug vor. Dies ist indes in dieser Allgemeinheit nicht zutreffend. Schon aus der von ihm beschriebenen Systemstruktur ergibt sich, dass der Beschwerdeführer die öffentlichen IP-Adressen seiner Kunden wenigstens für die Dauer der Kommunikation speichern muss, da er ansonsten die abgerufenen Datenpakete seinen Kunden gar nicht übersenden könnte. [...] Dementsprechend räumt der Beschwerdeführer in seiner Erwiderung auf die Stellungnahme des Bundesamts für Sicherheit in der Informationstechnik ein, dass die IP-Adressen in den programminternen Datenstrukturen gespeichert werden. […] Jedenfalls fallen die Daten beim Zugriff auf den überwachten E-Mail-Account an, sind der Telekommunikationsanlage des Beschwerdeführers wenigstens zeitweise bekannt und werden von dieser auch zur Herstellung einer erfolgreichen Kommunikation mit dem anfragenden Kunden benutzt. Es ist daher jedenfalls verfassungsrechtlich vertretbar anzunehmen, die Daten seien beim Beschwerdeführer vorhanden [...].«[23]

Im Nichtannahmebeschluss des Bundesverfassungsgerichts wird zwar anerkannt, dass bei *Posteo* das Sammeln sowie die Kenntnisnahme von Daten – wo es nur geht – vermieden, der Datenverarbeitungsgrundsatz der »Datensparsamkeit« sehr ernst genommen wird,[24] aber (eben auf theoretischer, technisch-faktischer Ebene) – nötigenfalls unter Veränderung der Infrastruktur – die IP-Adressen für Strafverfolgungszwecke protokolliert und herausgegeben werden *könnten*:

> »Dass der Beschwerdeführer auf die externen IP-Adressen – derzeit – nicht zugreifen kann, steht dem nicht entgegen. Denn dies liegt nicht daran, dass die Daten an sich nicht vorhanden wären, sondern allein daran, dass sich der Beschwerdeführer aus Datenschutzgründen dazu entschlossen hat, diese vor seinen internen Systemen zu verbergen und sie nicht zu protokollieren. Das Unterlassen einer entsprechenden Protokollierung ist indes



> nicht zwangsläufig [...], sondern allein dem vom Beschwerdeführer bewusst gewählten Geschäfts- und Systemmodell geschuldet. Dies wird nicht nur vom Bundesamt für Sicherheit in der Informationstechnik in seiner Stellungnahme bestätigt, […] sondern wird zudem durch den Vortrag des Beschwerdeführers belegt, wonach er sein System, wenn auch mit nicht unerheblichem technischen und finanziellen Aufwand, entsprechend umgestalten könnte.«[25]

Posteo könne sich nicht durch eine bestimmte Ausgestaltung des eigenen Geschäftsmodells rechtlichen Verpflichtungen, die der Strafverfolgung dienten, entziehen:

> »Zwar erscheint das Anliegen des Beschwerdeführers, ein datenschutzoptimiertes und daher für viele Nutzer attraktives Geschäftsmodell anzubieten, auch unter dem Gesichtspunkt des Art. 12 Abs. 1 GG grundsätzlich durchaus schützenswert. Dies kann ihn jedoch nicht von den im Rahmen einer vertretbaren Auslegung gewonnenen Vorgaben des TKG und der TKÜV, die dem verfassungsrechtlichen Erfordernis einer funktionstüchtigen Strafrechtspflege Rechnung tragen (vgl. BVerfGE 133, 168 <199 Rn. 57>; stRspr), entbinden.«[26]

Posteo machte im Zuge des Verfahrens immer wieder geltend, es sei aufgrund ihrer (derzeit) eingesetzten Infrastruktur nicht möglich, die IP-Adressen ihren KundInnen zugeordnet zu protokollieren und herauszugeben.[27] Zur Verdeutlichung: Posteo stritt nicht ab, dass IP-Adressen beim Zugriff der KundInnen auf ihre Postfächer Verwendung finden würden – das ist schließlich für die Kommunikation über das Internet eine notwendige Bedingung –, sondern lediglich, dass die eingesetzte Infrastruktur dazu in der Lage sei, die Verwendung findenden IP-Adressen den Postfächern ihrer KundInnen zugeordnet – und damit die IP-Adressen ihrer KundInnen – erfassen, protokollieren und damit den Ermittlungsbehörden herausgeben zu können. Bei dem Verfahren vor dem BVerfG ging es um zweierlei: zum einen, ob eine rechtliche Verpflichtung zur Protokollierung und Herausgabe KundInnen zuordenbarer IP-Adressen – bei Vorhandensein (!) beim Anbieter (also *Posteo*) – besteht, und im Anschluss daran, ob IP-Adressen von KundeInnen bei *Posteo* überhaupt vorhanden sind, diese also – bei nötigenfalls technischen Systemanpassungen – den KundInnen zugeordnet protokolliert und herausgegeben werden könnten und damit müssten.[28] Irgendwann erledigte sich die Überwachung des betreffenden Anschlusses und *Posteo* bezahlte das verhängte Ordnungsgeld.[29] *Posteo* kritisierte die Entscheidung des BVerfG und lehnt es bis heute zu ab, allgemein die IP-Adressen ihrer KundInnen zu protokollieren.[30]

Am 13.06.2019 erging dann beim Europäischen Gerichtshof (EuGH) das sogenannte ›*Gmail*-Urteil‹:[31] Aufgrund dieses Urteils sind E-Mail-Dienste wie *Gmail* – und so eben auch *Posteo* – nicht als »elektronischer Kommunikationsdienst« im Sinne des Art. 2 lit. c der Rahmenrichtlinie[32] anzusehen,[33] was zur Folge hat, dass die maßgeblichen streitgegenständlichen Normen[34] der ›*Posteo*-Entscheidung‹, welche zur Ermöglichung der Protokollierung und Herausgabe auf KundInnen bezogener IP-Adressen verpflichteten, keine Anwendung mehr finden.[35]

Vorläufig scheint die kundInnenbezogene IP-Adressen-Protokollierung bei *Posteo* somit abgewendet, es bleibt abzuwarten, was die (gesetzliche) Zukunft bringen wird.

Hinsichtlich der Inhaltsdatenverarbeitung weist *Posteo* aus:

> »Die Inhalte einer Kommunikation und ihren [sic] näheren Umstände (E-Mails und deren Metadaten) unterliegen dem Fernmeldegeheimnis (auch Telekommunikationsgeheimnis) und sind grundrechtlich geschützt. Das bedeutet: Niemand darf Ihre E-Mails lesen – und wir dürfen sie auch nicht an Dritte weitergeben. Das wäre eine Verletzung Ihrer Grundrechte und strafbar. Eingeschränkt werden kann das Fernmeldegeheimnis nur im Einzelfall und nur durch einen Richter, beim Verdacht auf bestimmte Straftaten.«

Dazu gilt es jedoch anzumerken, dass aufgrund des thematisierten EuGH-Urteils die Anwendbarkeit der telekommunikationsrechtlichen Normen, welche auch die Verpflichtung der Diensteanbieter zur Wahrung des Fernmeldegeheimnisses enthalten,[36] fraglich ist. Auf technischer Ebene werden die Inhaltsdaten bei *Posteo* mit neuesten Sicherheitstechnologien durch Verschlüsselung geschützt. Darüber hinaus ist hervorzuheben, dass *Posteo* keine personenbezogenen Daten an Drittunternehmen oder Dienstleister weitergibt, die Datenerhebung durch sogenannte Tracking-Cookies oder Tracking-Tools unterbleibt, insbesondere keine Social-Media-Plugins eingesetzt werden. Somit wird auch die oft unbemerkte Erhebung von Metadaten (insbesondere auch durch Dritte) vermieden.

Die Zusammenfassung der Datenschutzerklärung von *Startpage* wird man wohl kurz und übersichtlich nennen können: »In aller Kürze: Startpage.com erfasst oder teilt keine deiner persönlichen Informationen. Wir tracken dich nicht. Wir legen kein Profil von dir an. Punkt.« Natürlich führen sie im Folgenden noch Einzelheiten aus, alles in allem werden jedoch keinerlei personenbezogene Daten erhoben.

III. Über die Einhaltung des rechtlichen Rahmens hinaus

Welche Auswirkungen haben die Infrastrukturen, in denen wir uns im Internet bewegen, auf uns als Individuen und als Gesellschaft? Die Strukturierung digitaler Anwendungen hat erhebliche Auswirkungen: Die Freiheit ist zentraler Wert und Voraussetzung demokratischer Gesellschaften; der Austausch, das freie Kommunizieren und die freie Entfaltung der Einzelnen sind die Grundlage, die Ausbildung einer persönlichen Autonomie und eigenen Meinung, eines eigenen Selbstbildes ist zentral, um als freieR BürgerIn zu leben. Digitale Anwendungen beeinflussen somit erheblich die Freiheit der Einzelnen. Die Art, wie wir einander begegnen können, hängt stark davon ab, wie Kommunikationsumfelder aussehen. Um die Freiheit der BürgerInnen zu ermöglichen und zu schützen, braucht es eine geschützte individuelle Privatsphäre, denn »in liberalen Gesellschaften hat das Private die Funktion, ein autonomes Leben zu ermöglichen und zu schützen.«[37] Privatheit ist also die funktionale Bedingung für Freiheit im Sinne von Autonomie[38]:

> »[...] die eigentliche Realisierung von Freiheit, nämlich autonome Lebensführung, [ist] nur möglich [...] unter Bedingungen geschützter Privatheit; bestimmte Foren des praktischen Selbstverhältnisses – Deliberation über konfligierende Wünsche und Selbstbilder, über die Genese von Wünschen usf. –, als Bedingung autonomer Entscheidungen, und ein daraus resultierendes autonomes Leben und Verhalten – das Leben von ›Projekten‹ – sind als gelungene nur zu entwickeln, wenn es geschützte private Bereiche und Dimensionen des Lebens gibt.«[39]

Nur in einem geschützten Raum – ganz konkret gedacht als Zimmer oder Wohnung, aber auch als Raum im übertragenen Sinne – der dem Zugriff anderer entzogen ist, können wir unsere Persönlichkeit frei entfalten, eigene Entscheidungen treffen und *wir selbst* sein. Im Bereich des Internets und der Datenerhebung geht es vorwiegend um Privatheit auf einer informationellen Ebene, d. h. um persönliche Informationen über das Individuum.[40] Darüber *müsste* die Kontrolle beim autonomen Individuum liegen, diese scheint ihm allerdings immer mehr zu entgleiten. Doch sie ist zentral für die Einzelnen: Der Verlust der informationellen Privatheit führt zu einer Durchleuchtung der Individuen, ihrer Wünsche und Interessen, und schränkt ihre dezisionale Privatheit, also die Freiheit, Entscheidungen nach dem eigenen Abwägen und Dafürhalten ohne Einmischung anderer zu treffen, ein.[41] Wer mit ständiger Beobachtung und Überwachbarkeit lebt, verliert seine Freiheit, wird manipulierbar und steuerbar und wird sein eigenes Verhalten zunehmend Normen der Erwünschtheit anpassen.[42]

Was macht das Verhalten von *Posteo* nun so bemerkenswert? *Posteo* ermöglicht mit seinem E-Mail-Dienst eine Form der Kommunikation und des Austausches, in dem eine erhebliche Privatheit gewährleistet ist. Die Vehemenz, mit der *Posteo* seine Positionen vertritt und verteidigt, verdient dabei Beachtung. Es scheint dem Unternehmen nämlich nicht lediglich um die Ausschöpfung seines unternehmerischen Potenzials zu gehen, sondern um die Veränderung einer Kultur in Bezug auf Anwendungen und Dienstleistungen im Netz. Es stellt einen Gegenpol zur *Freemium*-Kultur dar, deren monetäre Kostenfreiheit durch einen erheblichen Datenabfluss erkauft wird. Hinzukommt, dass Daten, die einmal erhoben sind, nicht nur für ein Geschäftsmodell genutzt werden können, sondern auch zu Strafverfolgungs- oder gänzlich anderen Zwecken.

Zugegeben sei, dass die effektive Strafverfolgung ein wesentlicher Bestandteil des Rechtsstaates ist, das Ausmaß von Strafverfolgungsmaßnahmen jedoch mit notwendigen Privatheitsbedingungen der BürgerInnen in Konflikt geraten, ein ausgeglichenes Verhältnis in eine Disbalance mutieren kann. *Posteo* vertritt hier nach Kräften die Agenda eines unbedingten Privatsphäreschutzes, wie das Verfahren vor dem BVerfG gezeigt hat. *Posteo* verteidigt die Möglichkeit der KundInnen, privat und anonym zu blieben, indem möglichst keine Daten gesammelt werden. Das Unternehmen versucht also – seiner politischen Agenda folgend –, sich seinen KundInnen gegenüber loyal zu verhalten und die zugesicherten Schutzmechanismen aufrecht zu halten. Damit vertritt *Posteo* eine Verbindlichkeit, die über die Einhaltung des Rechtsrahmens hinausgeht, sowie Schutz und Fairness gegenüber den NutzerInnen verwirklicht. Dadurch, dass sich die Konsequenzen aus der ›*Posteo*-Entscheidung‹ in Folge des ›*Gmail*-Urteils‹ gewissermaßen erübrigt haben, kann *Posteo* diese Praxis (vorerst) weiterführen. Die Privatsphäre und Anonymität der NutzerInnen scheint für *Posteo* nicht verhandelbar oder aufgebbar. Man könnte daher sagen, dass das Unternehmen nicht nur Geschäfte macht, sondern auch ethische Standards hochhält und damit einen Anstand in die Digitalwirtschaft bringt, der dort sonst selten ist.

F. Alternativen: Was sie auszeichnet und warum man sie nutzen sollte

Was zeichnet nun unsere vorgestellten Alternativen aus? Zum einen, dass sie ihre Geschäftsmodelle und Motivationen transparent machen und – bestenfalls keine oder – eine nur geringe Motivation zur Verarbeitung von KundInnendaten haben, da sie sich auf anderen Wegen als durch deren Verarbeitung finanzieren. Darüber hinaus, dass sie ausweisen, *ob und welche* Datenverarbeitungen sowohl für die Verwendenden sichtbar als auch unsichtbar (im Hintergrund) stattfinden. Der Datenverarbeitungsgrundsatz der »Datenminimierung« ist in Art. 5 Abs. 1 lit. c DS-GVO verankert, demnach müssen personenbezogene Daten »dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt (›Datenminimierung‹)« sein. Unsere vorgestellten Alternativen haben sich diesem Grundsatz in einer dezidierten Art und Weise verschrieben. Der große Vorteil der Datenvermeidung ist, dass die Verarbeitung von Daten, die nicht erfasst worden sind, auch nicht durch Ge- oder Verbote geschützt werden müssen, sondern faktische Unmöglichkeit der Verwendung besteht – sozusagen das Spiegelbild der faktischen Ausschlussunmöglichkeit von Datenvervielfältigungen im Zeitalter digitaler Technologien. Daneben kennzeichnet die vorgestellten Alternativen, dass sie auf der Ebene ihrer Geschäftsmotivation dem Individuum, der Gesellschaft und einer freiheitlich-demokratischen Grundordnung – man denke beispielsweise an die Ermöglichung von Autonomievoraussetzungen, Meinungsbildung und den Schutz von Minderheiten – dienen.

Es gibt sie, Alternativen. Und das Erstaunliche ist: Es ist nichts Unerwartetes dabei gewesen, was die vorgestellten Alternativen ausmacht. Letztlich sind es Aspekte die schon ›der Volksmund‹ zu bedenken geben würde: Jeder weiß, »im Leben gibt es nichts umsonst.« Vielleicht lohnt es sich doch, einen gewissen Geldbetrag in bestimmte Dienste zu investieren. Denn »man sieht sich immer zweimal« – vielleicht gilt das auch für Informationen, die man schon vergessen geglaubt hatte und die einem später unangenehm sein können. Mit einer gesunden Portion Skepsis sollte einem klar sein, dass »nicht alles Gold ist, was glänzt« und hinter so manchem schicken Design und Marketing andere Dinge ablaufen, als man sich wünschen würde. Lassen Sie sich jedoch nicht entmutigen, wenn Sie Alternativen bisher keine Aufmerksamkeit geschenkt haben: »Erkenntnis ist der erste Weg zur Besserung«. In kleinen Schritten lassen sich diese vielleicht in Ihre Internetnutzungsgewohnheiten implementieren, »Rom wurde auch nicht an einem Tag erbaut«: Zuerst der Wechsel der Standardsuchmaschine, dann das Einrichten eines zweiten E-Mail-Postfaches, dann der schrittweise Umzug zu dem neuen E-Mail-Postfach, schließlich vielleicht sogar noch die Verwendung eines alternativen Messenger-Dienstes, indem man sich mit seinem Freundes-/Bekannten- oder KollegInnenkreis auf eine Alternative einigt. »Der stete Tropfen höhlt den Stein«: Ob der ›Stein‹ nun unsere Privatsphäre oder die Marktmacht der großen Internetkonzerne ist, das ist auch unsere Entscheidung, die Entscheidung der VerbraucherInnen.

Lea Watzinger

Wissenschaftliche Mitarbeiterin am DFG-Graduiertenkolleg »Privatheit und Digitalisierung«.

Felix Sobala

War von 2016 bis 2019 Wissenschaftlicher Mitarbeiter am DFG-Graduiertenkolleg »Privatheit und Digitalisierung«.

Endnoten

1 Siehe hierzu auch den Sammelband Aldenhoff et al. (Hg.): *Digitalität und Privatheit*. Bielefeld: transcript 2019.
2 Vgl. beispielhaft zum (tatsächlichen) Ausmaß der Datenverarbeitung durch die App *Runtastic* Ochs, Carsten: o.A. In: Berger, Franz/Deremetz, Anne/Hennig, Martin/Michell, Alix (Hg.): *Verantwortung in digitalen Kulturen. Privatheit im Geflecht von Medien, Recht, Gesellschaft.* Verlag: o.A.
3 So fordert Art. 12 Abs. 1 S. 1 DS-GVO: »Der Verantwortliche trifft geeignete Maßnahmen, um der betroffenen Person alle Informationen [...], die sich auf die Verarbeitung beziehen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln [...].«
4 Siehe zur Prävalenz von zwischen dystopisch und utopisch changierenden Färbungen derartiger Diskurse Hennig, Martin/Kelsch, Jakob/Sobala, Felix: *›Smarte Diktatur‹ oder ›egalitäre Netzgemeinschaft‹?*. In: Aldenhoff, Christian/Edeler, Lukas/Hennig, Martin/Kelsch, Jakob/Raabe, Lea/Sobala, Felix (Hg.): *Digitalität und Privatheit*. Bielefeld: transcript 2019, S. 11–21, sowie Piegsa, Miriam/Trost, Kai Erik: *Privatheit in der digitalen Gesellschaft. Von Fragen der Subjektbildung und ethischen Grenzbereichen, Veränderungen sozialer Beziehungen und rechtlichem Regulierungsbedarf*. In: Burk, Steffen/Hennig, Martin/Heurich, Benjamin / Klepikova, Tatiana/Piegsa, Miriam/Sixt, Manuela/ Trost, Kai Erik (Hg.): *Privatheit in der digitalen Gesellschaft*. Berlin: Duncker & Humblot 2018, S. 8–13.
5 Die Website des Unternehmens ist abrufbar unter: https://posteo.de/. Alle folgenden *Posteo* betreffenden Aussagen und Zitate sind folgenden Websites entnommen: *Wir über uns*. Online: https://posteo.de/site/ueber_posteo; *Maximaler Datenschutz*. Online: https://posteo.de/site/datenschutz; *Anonymisierte Zahlung*. Online: https://posteo.de/site/bezahlung; *Datenschutzerklärung* 2019. Online: https://posteo.de/site/datenschutzerklaerung; *Posteo-Transparenzbericht*. Online: https://posteo.de/site/transparenzbericht; betreffend den Prüfbericht der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit Voßhoff, Andrea: *Beratungs- und Kontrollbesuch E-Mail Posteo. Bericht* 2016. Online: https://posteo.de/bfdi_pruefbericht.pdf (jeweils 04.09.2019).
6 Die Website der Suchmaschine ist abrufbar unter: https://www.startpage.com/. Alle folgenden *Startpage* betreffenden Aussagen und Zitate sind folgenden Websites entnommen: Über uns 2019: Online: https://www.startpage.com/de/about-us.html; *Unsere Datenschutzrichtlinien* 2019. Online: https://www.startpage.com/de/search/privacy-policy.html; *Pressezentrum* 2019. Online: https://www.startpage.com/blog-de/pressezentrum/ (jeweils 04.09.2019).
7 Ein E-Mail-Postfach bei *Posteo* inklusive Adressbuch- und Kalenderfunktion kostet 1€/Monat, das Postfach enthält standardmäßig 2 GB Speicherplatz, zwei Alias-Adressen und drei Kalender. Zusätzliche Leistungen lassen sich dann noch dazubuchen (siehe Posteo: *Das Postfach. Alle Leistungen*. Online: https://posteo.de/site/leistungen (04.09.2019)).
8 Siehe zum Ursprung dieser Bezeichnung Fred Wilson in seinem Blog, dort hatte er das zugrundeliegende Geschäftsmodell beschrieben und zu Namensvorschlägen aufgerufen (siehe Wilson, Fred: *My Favorite Business Model*. In: *AVC* vom 23.03.2006. Online: https://avc.com/2006/03/my_favorite_bus/ (04.09.2019)), aus den Vorschlägen wählte er diesen von Jarid Lukin stammenden Vorschlag als passende Bezeichnung aus (Wilson, Fred: *The Freemium Business Model.* In: *AVC* vom 23.03.2006. Online: https://avc.com/2006/03/the_freemium_bu/ (04.09.2019)).
9 Zumindest werden die mit Basisfunktionen ausgestatteten Anwendungsversionen ohne Gegenleistung in Geld angeboten. Zum Vergleich: Für das *FreeMail*-Postfach von *WEB.DE* ist kein Entgelt in Form von Geld zu entrichten, zu diesem gehören ebenfalls ein Kalender und ein Adressbuch, zusätzlich auch Online-Speicherplatz in der Cloud, es können sogar Office-Dateien im Postfach online bearbeitet werden. Standardmäßig gehören 2GB Online-Speicherplatz zu diesem kostenlosen E-Mail-Postfach, für das Herunterladen beziehungsweise Verwenden von *WEB.DE*-Anwendungen erhält man bis zu 8GB weiteren Speicherplatz. Darüber hinaus kann kostenpflichtig (für Geld) Speicherplatz dazugebucht werden (siehe WEB.DE: *FreeMail*. Online: https://web.de/email/#.pc_page.produktseiten.cloud.footer_1.freemail (04.09.2019)).
10 Siehe Posteo: *Datenschutzerklärung*. Online: https://posteo.de/site/datenschutzerklaerung (04.09.2019): »Wir arbeiten unabhängig und haben keine Werbepartner: Nur so kann ein Internetdienst tatsächlich datenschutzfreundlich betrieben werden. [...] Wir geben zu keinem Zeitpunkt personenbezogene Daten an Dritt-Unternehmen oder Dienstleister weiter. Alle Daten werden ausschliesslich [sic] in Deutschland auf unseren Servern gespeichert. Posteo ist Kunden-finanziert: Werbepartner oder Investoren gibt es nicht.«
11 Siehe hierzu zum Beispiel die Veröffentlichungen des Prüfberichtes der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, Andrea Voßhoff, aus dem Jahre 2016 (Voßhoff, Andrea: *Beratungs- und Kontrollbesuch E-Mail Posteo. Bericht* 2016. Online: https://posteo.de/bfdi_pruefbericht.pdf (04.09.2019)) sowie des *Posteo*-Transparenzberichtes (Posteo: *Posteo-Transparenzbericht*. Online: https://posteo.de/site/transparenzbericht (04.09.2019)).
12 Verschlüsselung von Daten mag zwar eine gewisse zusätzliche Sicherheit vor der unautorisierten Datenverwendung bieten, dennoch sollte man sich immer bewusstmachen, dass jede Verschlüsselung theoretisch (denknotwendig) auch wieder entschlüsselt werden kann, ansonsten würde es sich ja nicht um ein ›Verschlüsseln‹, sondern um ein Löschen beziehungsweise Überschreiben – und damit ein ›Unbrauchbarmachen‹ – der betreffenden Daten handeln.
13 Wir verwenden hier die Einteilung nach der rechtlichen Terminologie. Für einen kurzen Überblick über diese Kategorisierung von Daten im Recht wie auch eine (andere) Kategorisierung in der Wirtschaftsinformatik siehe Czernik, Agnieszka: Definition und Unterscheidung der Begriffe Daten, Informationen & Wissen. In: *Datenschutzbeauftragter INFO* vom 05.08.2016. Online: https://www.datenschutzbeauftragter-info.de/definition-und-unterscheidung-der-begriffe-daten-informationen-wissen/ (04.09.2019).
14 Telemediendienste werden (insbesondere) durch das TMG reguliert, Telekommunikationsdienste durch das TKG. Von einer genaueren Darstellung und Differenzierung dieser beiden Regulierungsgegenstände wird aufgrund des Beitragszieles, der Verschaffung eines Überblicks, abgesehen. Für Interessierte sei jedoch darauf hingewiesen, dass im Rahmen des ›*Gmail*-Urteils‹, welches noch später thematisiert werden wird, genau diese Differenzierung – ob es sich bei *Gmail* beziehungsweise bei *Posteo* um einen Telekommunikationsdienst oder einen Telemediendienst handelt – von entscheidender Bedeutung ist.
15 Mit dieser Unterscheidung ist gemeint, dass im Kontext von Kommunikationsanwendungen – wie zum Beispiel einem E-Mail-Postfach – mit ›Metadaten‹ nicht nur die Daten bezeichnet werden, die durch die Nutzung auf Anwendungsebene – also des E-Mail-Postfaches – bedingt sind, sondern auch solche, die die näheren Umstände der Kommunikation – also der jeweiligen E-Mail, wie zum Beispiel AbsenderIn, EmpfängerIn, Datum etc. – beschreiben. So kann es dann auch kommen, dass im Kommunikationszusammenhang auch auf der Ebene der Inhaltsdaten von ›Metadaten‹ die Rede ist, nämlich hinsichtlich der Umstände des jeweiligen Kommunikationsaktes.
16 Czernik, Agnieszka: Metadaten – Wer, wann, mit wem, wie lange. In: *Datenschutzbeauftragter INFO* vom 27.11.2015. Online: https://www.datenschutzbeauftragter-info.de/metadaten-wer-wann-mit-wem-wie-lange/ (04.09.2019).
17 Siehe dazu schon im Zuge des Diskurses um die Vorratsdatenspeicherung Biermann, Kai: Was Vorratsdaten über uns verraten.

In: *ZEIT ONLINE* vom 24.02.2011. Online: https://www.zeit.de/digital/datenschutz/2011-02/vorratsdaten-malte-spitz/komplettansicht (04.09.2019).
18 Was die im Folgenden nicht konsequente Verwendung der terminologischen Unterscheidung von *Nutzungs-* respektive *Verkehrsdaten* anbelangt, so gilt es zu beachten, dass es sich in Folge eines Urteils des Europäischen Gerichtshofes (EuGH 2019: *Urt. v. 13.06.2019 – C-193/18*; siehe zu diesem Urteil noch weiter unten und ausführlich die Urteilsbesprechung von Patrick Herget in diesem Magazin) bei E-Mail-Diensten, wie beispielsweise *Posteo*, nicht um Telekommunikations-Anbieter nach dem (bisher in Deutschland für einschlägig gehaltenen) TKG handelt (siehe schon Fn. 14) und es in Folge dessen zu inaktualitätsbedingten terminologischen Unstimmigkeiten bei Zitaten kommt.
19 *Posteo* erhebt nach eigenen Angaben weder Bestands- noch Verkehrsdaten wie beispielsweise IP-Adressen (»Wir erheben Ihre IP-Adresse nicht, wenn Sie unsere Website besuchen. [...] Wir erheben weder Bestandsdaten, noch verfügen wir über Verkehrsdaten (wie IP-Adressen) mit Postfachbezug.«, Posteo: Maximaler Datenschutz 2019. Online: https://posteo.de/site/datenschutz (04.09.2019)). In ihrem Prüfbericht vom 30.12.2016 führte die damalige Bundesdatenschutzbeauftragte für den Datenschutz und die Informationsfreiheit, Andrea Voßhoff, aus: »IP-Adressen von Kunden sind in den internen Systemen von Posteo nicht verfügbar und können daher auch nicht gespeichert werden. Innerhalb der Posteo-Server werden ausschließlich interne IP-Adressen verwendet, d.h. kein interner Server sieht eine externe IP-Adresse« (Voßhoff 2016, S. 5). Zusammenfassend stellt sie fest, »dass Posteo keine auf Kunden beziehbare IP-Adressen und damit keine Verkehrsdaten nach § 96 TKG zur Diensterbringung benötigt und speichert« (Voßhoff 2016, S. 6).
20 »Bestandsdaten oder personenbezogene IP-Adressen liegen zu Posteo-Postfächern nicht vor und können nicht herausgegeben werden.« (Posteo: *Datenschutzerklärung* 2019. Online: https://posteo.de/site/datenschutzerklaerung (04.09.2019)).
21 BVerfG: *Nichtannahmebeschluss v. 20.12.2018 – 2 BvR 2377/16*. Für einen kurzen Verfahrensüberblick siehe Wöbbeking, Maren: BVerfG: Verfassungsgemäße Verpflichtung zur Übermittlung von Internetprotokolladressen. In: *Computer und Recht (CR)* 2019, R28.
22 Vgl. die Rechtsansichten im Vorhinein sowie die Stellungnahmen im Rahmen des Verfassungsbeschwerdeverfahrens: BVerfG 2018, juris: Rz. 5–11, 16–30.
23 BVerfG 2018, juris: Rz. 48.
24 Das BVerfG beschreibt *Posteo* zu Beginn des Nichtannahmebeschlusses folgendermaßen (BVerfG 2018, juris: Rz. 2): »Der Dienst wirbt mit einem besonders effektiven Schutz der Kundendaten und sieht sich den Grundsätzen der Datensicherheit und der Datensparsamkeit verpflichtet. Er erhebt und speichert Daten nur dann, wenn dies aus technischen Gründen erforderlich oder – aus seiner Sicht – gesetzlich vorgesehen ist.«
25 BVerfG 2018, juris: Rz. 49.
26 BVerfG 2018, juris: Rz. 50.
27 »Der Beschwerdeführer wies jedoch darauf hin, dass Verkehrsdaten der Nutzer nicht ›geloggt‹ würden und solche Daten inklusive der IP-Adressen deshalb nicht zur Verfügung gestellt werden könnten.« (BVerfG 2018, juris: Rz. 5); »Dem widersprach der [...] Beschwerdeführer [...]. Die fraglichen IP-Adressen würden [...] nicht erhoben und seien auch nicht vorhanden.« (BVerfG 2018, juris: Rz. 6); »Der Annahme, die IP-Adressen seien [...] vorhanden, widersprach der Beschwerdeführer [...] unter Darstellung seiner Systemstruktur. [....] [Er] trenne sein internes Netz über ein sogenanntes NAT-Verfahren (Network Adress Translation), bei dem die Adressinformationen in Datenpaketen automatisiert durch andere ersetzt würden, aus Sicherheitsgründen strikt vom Internet ab. Die IP-Adressen der Kunden würden daher bereits an den Außengrenzen des Systems verworfen und seien dem Zugriff des Beschwerdeführers entzogen.« (BVerfG 2018, juris: Rz. 8); »Die IP-Adressen fielen hier indes nicht unter den Begriff [bereits angefallener oder zukünftig anfallender] Verkehrsdaten, da sie [...] nicht erhoben, verarbeitet oder genutzt würden. [...] Der Beschwerdeführer habe die verlangten Daten nicht und können sie auch nicht kurzfristig, sondern nur durch eine aufwändige Neustrukturierung seines EDV-Systems erfassen.« (BVerfG 2018, juris: Rz. 10); siehe zu den unterschiedlichen Ansichten insgesamt schon oben Fn. 22.
28 Vgl. BVerfG 2018, juris: Rz. 41–52, insbesondere Rz. 45–50.
29 Vgl. BVerfG 2018, juris: Rz. 14.
30 Vgl. Posteo: Erster Kommentar zur Entscheidung des Bundesverfassungsgerichts 2019. Online: https://posteo.de/blog/erster-kommentar-zur-entscheidung-des-bundesverfassungsgerichts (04.09.2019). Dort positioniert sich Posteo folgendermaßen: »Sollte es rechtlich keine weiteren Optionen mehr geben, werden wir unsere System-Architektur anpassen müssen, dabei jedoch eine Lösung wählen, die die Sicherheit und die Rechte unserer Kundinnen und Kunden nicht beeinträchtigt. Und, um es ganz klar zu sagen: Wir werden nicht damit beginnen, die IP-Adressen unserer unbescholtenen Kundinnen und Kunden zu loggen. Ein konservativer System-Umbau ist für uns keine Option. Es geht darum, bei richterlich angeordneten Telekommunikations-Überwachungen eine IP-Adresse zu einem betroffenen Postfach erheben zu können. Jegliche Änderungen werden wir transparent und nachprüfbar kommunizieren und dokumentieren.«
31 EuGH 2019: *Urt. v. 13.06.2019 – C-193/18*. Siehe zu diesem Urteil ausführlich die Urteilsbesprechung von Patrick Herget in diesem Magazin.
32 Richtlinie 2002/21/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste (Rahmenrichtlinie) (ABl. 2002, L 108, S. 33) in der durch die Richtlinie 2009/140/EG des Europäischen Parlaments und des Rates vom 25. November 2009 (ABl. 2009, L 337, S. 37, berichtigt im ABl. 2013, L 241, S. 8) geänderten Fassung.
33 Vgl. EuGH 2019, Rz. 35–38, 41.
34 Siehe zu den die Verpflichtung konkret enthaltenden Vorschriften BVerfG 2018, juris: Rz. 46f.
35 *Posteo* selber schreibt dazu in einem Hinweisbanner vor ihrem Transparenzbericht (Posteo: Wichtiger aktueller Hinweis. Online: https://posteo.de/site/transparenzbericht (04.09.2019)): »In Folge eines Urteils des Europäischen Gerichtshofes vom 13.06.2019 fallen E-Mail-Dienste wie Posteo nicht mehr unter die Pflichten des TKG. Alle Verweise auf das Telekommunikationsgesetz (TKG) auf diesen Seiten sowie die Bezeichnung von Posteo als ›Telekommunikations-Anbieter nach dem TKG‹ sind daher nicht mehr aktuell.« Dort auch zum Folgenden.
36 Siehe schon Fn. 14 und 18. Die Verpflichtung der Telekommunikationsdiensteanbieter zur Wahrung des Fernmeldegeheimnisses ergibt sich aus § 88 TKG, die Strafbarkeit bei Verletzung des Fernmeldegeheimnisses aus § 206 StGB.
37 Rössler, Beate: *Der Wert des Privaten*. Frankfurt am Main: Suhrkamp 2001, S. 10.
38 Vgl. Rössler 2001, S. 127.
39 Rössler 2001, S. 137.
40 Vgl. Rössler 2001, Kap. IV.2.
41 Vgl. Rössler 2001, S. 153ff.
42 Vgl. Rössler 2001, v.a. S. 218, zudem sei auf Michel Foucaults einschlägige Beobachtungen zu Panoptismus und Selbstkontrolle verwiesen: Foucault, Michel: *Überwachen und Strafen. Die Geburt des Gefängnisses.* Frankfurt am Main: Suhrkamp 1977.

Regulierung von *Over-the-Top*-Kommunikation

Der EuGH entscheidet, dass *Gmail* nicht als elektronischer Kommunikationsdienst eingestuft werden kann

Foto: Rcfotostock / stock.adobe.com

von Patrick Herget

In June 2019, the Court of Justice of the European Union issued two long-awaited rulings concerning the applicability of the European telecommunication framework and its regulations to internet-based communication services. While *SkypeOut* is considered an electronic communication service, the said regulations do not apply to *Gmail* because, as such, it does not convey signals »wholly or mainly«. The responsibility for the conveyance of signals became the decisive criterion, which relates *SkypeOut* to the telecommunication framework because it enables telephone calls to landline or mobile numbers using Voice-over-IP services and, therefore, carries responsibility along with the affiliated providers.

Mit einem aufsehenerregenden Urteil hat der Europäische Gerichtshof (EuGH) am 13.06.2019 entschieden, dass Googles internetbasierter E-Mail-Dienst, *Gmail*, keinen Telekommunikationsdienst im Sinne der europäischen Rahmenrichtlinie für elektronische Kommunikationsnetze und -dienste 2002/21/EG darstellt.[1] Bislang war umstritten, ob sogenannte *Over-the-Top* (*OTT*)-Kommunikationsdienste, die Leistungen über das Internet anbieten und dabei die vorhandene Infrastruktur eines Internetdienstanbieters nutzen, als elektronische Kommunikationsdienste im Sinne der Richtlinie eingeordnet werden können und somit den sektorspezifischen Regulierungen des Telekommunikationsrechts unterfallen.[2]

Einführung

Art. 2 lit. c RL 2002/21/EG definiert elektronische Kommunikationsdienste als »gewöhnlich gegen Entgelt erbrachte Dienste, die ganz oder überwiegend in der Übertragung von Signalen über elektronische Kommunikationsnetze bestehen, einschließlich Telekommunikations- und Übertragungsdienste in Rundfunknetzen. Ausgenommen sind dabei jedoch Dienste, die Inhalte über elektronische Kommunikationsnetze und -dienste anbieten oder eine redaktionelle Kontrolle über sie ausüben; nicht dazu gehören die Dienste der Informationsgesellschaft im Sinne von Artikel 1 der Richtlinie 98/34/EG, die nicht ganz oder überwiegend in der Übertragung von Signalen über elektronische Kommunikationsnetze bestehen«.

OTT-Dienste hingegen sind »weder legaldefiniert noch ist die Bezeichnung ›*OTT*‹ überhaupt ein Rechtsbegriff.«[3] Legt man eine Definition des Gremiums Europäischer Regulierungsstellen für elektronische Kommunikation (GEREK) zugrunde, so handelt es sich bei *OTT*-Angeboten um »content, a service or an application that is provided to the end user over the public Internet.«[4] Folglich stellt alles, was über das offene Internet transportiert wird, einen *OTT*-Dienst dar.[5] Grundsätzlich wird dabei zwischen *OTT*-Kommunikationsdiensten (Voice- und Video-over-IP, Instant Messaging, E-Mail-Dienste) und *OTT*-Inhaltsdiensten (z. B. Videoplattformen, Cloud-Dienste) differenziert. Im Kontext dieses Beitrages sind lediglich *OTT*-Kommunikationsdienste von Bedeutung, die eine Individualkommunikation zwischen den NutzerInnen ermöglichen. *OTT*-Kommunikationsdienste können grob in die bereits erwähnten Kategorien E-Mail-Dienste, Instant Messaging-Dienste und Voice- und Video-over-IP-Dienste eingeteilt werden, wobei oftmals eine Kombination verschiedener Elemente im Rahmen eines Dienstes stattfindet.[6] Darüber hinaus kann unterschieden werden, ob diese Dienste über einen Server des Dienstanbieters abgewickelt werden (*Client-Server*-Modelle) oder ob eine direkte Verbindung zwischen den KommunikationsteilnehmerInnen existiert (*Peer-to-Peer*-Modelle).[7] Die rechtliche Einordnung von *OTT*-Kommunikationsdiensten war bislang umstritten, da diese sowohl Inhalte bereitstellen und auch (zumindest teilweise) an der Signalübertragung beteiligt sind.[8] So existierten bisher unterschiedliche Regelungsansätze innerhalb der Europäischen Union für die rechtliche Einordnung von *OTT*-Diensten. Bislang wurde etwa in Finnland ein E-Mail-Dienst als Telekommunikationsdienst klassifiziert, wenn der Anbieter an der Übertragung von Signalen beteiligt ist, während diese Einstufung in den Niederlanden mit der Begründung, dass der Anbieter die Signale nicht selbst überträgt, bisher verneint wurde.[9] Entscheidend für die Einordnung von *OTT*-Kommunikationsdiensten ist demnach die Frage, ob diese ganz oder überwiegend in der Übertragung von Signalen über elektronische Kommunikationsnetze bestehen. Im Rahmen des *Gmail*-Vorlageverfahrens nutzte der EuGH nun die Gelegenheit, um dieses Kriterium zu konkretisieren. In Zusammenschau mit dem kurz zuvor ergangenen Urteil im *SkypeOut*-Vorabentscheidungsersuchen[10] ergeben sich nun präzise Kriterien für die Anwendbarkeit des Telekommunikationsrechts.

Oberverwaltungsgericht Münster befragt EuGH

Ausgangspunkt des Verfahrens stellte ein Bescheid der Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (BNetzA) nach § 126 des Telekommunikationsgesetzes (TKG) aus dem Jahr 2012 dar, in dem festgestellt wurde, dass es sich bei *Gmail* um einen Telekommunikationsdienst gem. § 3 Nr. 24 TKG handle und der E-Mail-Dienst deshalb der Meldepflicht gem. § 6 TKG nachkommen müsse.[11] § 6 TKG verpflichtet die gewerblichen Betreiber öffentlich zugänglicher Kommunikationsnetze und die gewerblichen Erbringer öffentlich zugänglicher Kommunikationsdienste, die Aufnahme, Änderung und Beendigung ihrer Tätigkeit sowie Änderungen seiner Firma unverzüglich bei der BNetzA zu melden. Darüber hinaus sind elektronische Telekommunikationsdienste an die bereichsspezifischen Vorschriften des TKG etwa in Bezug auf Datenschutz gem. § 91 ff. TKG und die öffentliche Sicherheit gem. § 108 ff. TKG gebunden. So haben Sicherheitsbehörden mit richterlichem Beschluss Zugriff auf herkömmliche SMS, bisher aber nicht auf *OTT*-Dienste. Als Telekommunikationsdienst wäre *Gmail* unter anderem dazu verpflichtet, Schnittstellen für den Zugriff der Ermittlungsbehörden einzurichten. Google wandte sich gegen den Bescheid der BNetzA. Nachdem das Widerspruchsverfahren erfolglos blieb, erhob Google Klage beim Verwaltungsgericht (VG) Köln, die jedoch am 11.11.2015 abgewiesen wurde. Das VG begründete seine Entscheidung damit, dass der Umstand, dass die Signalübertragung nicht durch Google selbst, sondern durch die beteiligten Internet-

Provider erfolge bzw. über das offene Internet stattfinde, für die Einordnung des Dienstes nicht entscheidend sei, da die einzelnen Prozessschritte nicht getrennt bewertet werden könnten; darüber hinaus hindere die für NutzerInnen kostenfreie Nutzbarkeit des Dienstes nicht die Annahme der Gewerblichkeit des Dienstes.[12] Die regelmäßige Entgeltlichkeit des Dienstes wurde dabei insbesondere aufgrund der Werbefinanzierung bejaht.[13] Auch einer Verantwortlichkeit für die »Signalübertragungs-(Vor-)leistung«[14] Googles gegenüber den NutzerInnen stimmte das VG zu, da sich Google die Signalübertragungsleistung durch Anbieten eines Kommunikationsdienstes zu eigen mache.[15] Darüber hinaus gäben NutzerInnen durch die Sendeeingabe den entscheidenden Impuls zur Signalübertragung.[16] Google erbringe mit *Gmail* somit einen Telekommunikationsdienst im Sinne von § 3 Nr. 24 TKG und unterliege dementsprechend auch der Meldepflicht, weshalb der BNetzA die Überwachung der Tätigkeit auf dem Markt, vor allem auch im Hinblick auf Erfordernisse der öffentlichen Sicherheit sowie des Kunden- und Datenschutzes, ermöglicht werden müsse.[17]

Im Folgenden legte Google Berufung gegen das Urteil beim Oberverwaltungsgericht (OVG) Münster ein.[18] Google machte dabei geltend, dass *Gmail* kein Telekommunikationsdienst sei, da keine Signale durch den Dienst selbst übertragen würden. *Gmail* setze zwar eine Signalübertragung voraus, diese erfolge aber nicht durch Google selbst, sondern – sowohl für die Datenübermittlung zwischen den NutzerInnen von *Gmail* und den E-Mail-Servern von Google als auch für die Datenübermittlung zwischen den E-Mail-Servern von Google und den E-Mail-Servern anderer E-Mail-Dienste – durch die Internetzugangsanbieter.[19] Die Signalübertragungsleistung sei Google darüber hinaus auch nicht zurechenbar, weil die Signalübertragung über das offene Internet nach dem *Best-Effort*-Prinzip[20] erfolge.[21] Daher könne weder eine tatsächliche noch eine rechtliche Kontrolle über den Vorgang der Signalübertragung ausgeübt werden.[22]

Im weiteren Verlauf setzte das OVG das Verfahren aus und ersuchte den EuGH um Vorabentscheidung folgender drei Fragen,[23] da die Definition für Telekommunikationsdienste aus § 3 Nr. 24 TKG auf die Bestimmung gem. Art. 2 lit. c RL 2002/21/EG zurückgeht: (1) »Ist das Merkmal ›Dienste, die ganz oder überwiegend in der Übertragung von Signalen über elektronische Kommunikationsnetze bestehen‹ aus Art. 2 Buchst. c der Rahmenrichtlinie dahin auszulegen, dass es auch internetbasierte E-Mail-Dienste erfasst oder erfassen kann, die über das offene Internet bereitgestellt werden und selbst keinen Internetzugang vermitteln?« (2) Im Falle einer Bejahung: »Kann das Merkmal gleichwohl ausnahmsweise dann erfüllt sein, wenn der Erbringer eines solchen Dienstes zugleich einige eigene mit dem Internet verbundene elektronische Kommunikationsnetze betreibt, die jedenfalls auch für die Zwecke des E-Mail-Dienstes genutzt werden können? Unter welchen Voraussetzungen ist dies gegebenenfalls möglich?« (3) »Wie ist das Merkmal ›gewöhnlich gegen Entgelt erbracht‹ aus Art. 2 Buchst. c der Rahmenrichtlinie auszulegen?«

Schwerpunkt Signalübertragung?

Die ersten beiden Vorlagefragen wurden vom EuGH zusammen geprüft, wobei das Merkmal der ganz oder überwiegenden Signalübertragung im Zentrum stand. Der Gerichtshof stellte dabei zunächst fest, dass *Gmail* zwar grundsätzlich eine Signalübertragung vornimmt, indem in Datenpakete zerlegte E-Mails über ihre E-Mail-Server eingespeist und empfangen werden.[24] Einen elektronischen Kommunikationsdienst gem.

Foto: Krisana / stock.adobe.com

Art. 2 lit. c RL 2002/21/EG stelle *Gmail* dennoch nicht dar, da dieser Dienst nicht ganz oder überwiegend in der Übertragung von Signalen über elektronische Kommunikationsnetze bestehe.[25] Unter Bezugnahme auf das *UPC DTH*-Urteil[26] vom 30.04.2014 wird dabei die Verantwortlichkeit zum zentralen Kriterium des EuGH dafür, ob ein Dienst ganz oder überwiegend aus der Übertragung von Signalen besteht. Die Verantwortlichkeit der Signalübertragung beim Versenden einer E-Mail liege einerseits bei den Internetzugangsanbietern von AbsenderInnen und EmpfängerInnen sowie gegebenenfalls bei den Anbietern von internetbasierten E-Mail-Diensten und den Betreibern öffentlicher Kommunikationsnetze.[27] Dass der Erbringer eines internetbasierten E-Mail-Dienstes bei Versendung und Empfang von Nachrichten aktiv tätig werde, reiche jedoch nicht für die Einstufung des Dienstes als elektronischen Kommunikationsdienst gem. Art. 2 lit. c RL 2002/21/EG aus.[28] Eine Verantwortlichkeit von Google gegenüber den InhaberInnen eines *Gmail*-Kontos bei der Übertragung der für das Funktionieren des Dienstes erforderlichen Signale bestehe demnach nicht, weshalb *Gmail* nicht als elektronischer Kommunikationsdienst im Sinne von Art. 2 lit. c RL 2002/21/EG eingeordnet werden könne.[29] Die Schwelle der ganz oder überwiegenden Signalübertragung ist im Fall von *Gmail* somit noch nicht überschritten. Der Umstand, dass Google auch eigene elektronische Kommunikationsnetze in Deutschland betreibe, sei nicht geeignet, dieses Ergebnis in Frage zu stellen.[30] Die dritte Vorlagefrage in Bezug auf die Entgeltlichkeit der Dienste ließ der EuGH in Anbetracht der Antwort auf die erste und zweite Frage unbeantwortet.[31]

Niederlage für die BNetzA

Im Gegensatz zu klassischen Netzbetreibern unterliegt *Gmail* somit weiterhin nicht der Meldepflicht aus § 6 TKG und muss darüber hinaus auch nicht den telekommunikationsrechtlichen Bestimmungen in Bezug auf die Gewährleistung der öffentlichen Sicherheit und des Datenschutzes nachkommen. Weitreichende Konsequenzen bleiben somit aus. Im Vorfeld der Entscheidung war befürchtet worden, dass die BNetzA im Falle einer Klassifizierung von *OTT*-Diensten als elektronische Kommunikationsdienste zu einer ›Megabehörde‹ hätte werden können, da sie dann enormen Einfluss auf Fragen des Datenschutzes und der Datensicherheit im Bereich des Internets gehabt hätte.[32] Sicherheitsbehörden hätten Daten gem. § 111 TKG herausverlangen können und Anbieter hätten ihre Systeme gem. § 18 TKG so ausgestalten müssen, dass Kommunikationsvorgänge mit anderen Plattformen ermöglicht worden wären.[33] Hätte die BNetzA den Prozess gegen Google gewonnen, so wäre dies vermutlich der Auftakt für Verfahren gegen weitere Anbieter gewesen.[34]

Andere Entscheidung im Fall *SkypeOut*

Die Frage, ob ein *OTT*-Dienst die rechtlichen Anforderungen für elektronische Kommunikationsdienste erfüllen muss, war nicht nur Gegenstand des aktuellen *Gmail*-Urteils, sondern wurde zuletzt auch im Rahmen des *SkypeOut*-Urteils thematisiert, wobei der EuGH den Dienst *SkypeOut* als elektronischen Kommunikationsdienst einstufte. Ähnlich wie im Fall von *Gmail* ging es im *SkypeOut*-Ausgangsverfahren darum, dass Skype Communications vom Belgischen Institut für Post und Fernmeldewesen *(IBPT)* gem. den Bestimmungen des belgischen Gesetzes über die elektronische Kommunikation aufgefordert wurde, seine Dienste zu melden und das Meldeformular beizufügen.[35] Jedoch existieren wesentliche Unterschiede zwischen den beiden *OTT*-Kommunikationsdiensten.

Zunächst ist die Nutzung von *SkypeOut* für UserInnen kostenpflichtig.[36] Darüber hinaus bietet *SkypeOut* im Gegensatz zu reinen *OTT*-Diensten die Möglichkeit, Voice-over-IP-Telefonate zu Festnetz- und Mobilfunknummern zu führen.[37] Ebenfalls unter Rückbezug auf das *UPC DTH*-Urteil macht der Gerichtshof dabei das Kriterium der Verantwortlichkeit bei *SkypeOut* daran fest, dass bei der Weiterleitung von Sprachsignalen zwischen Internet und dem Telefonnetz (*PSTN*) eine Gateway-Verbindung notwendig sei. Somit finde die Signalübertragung zunächst im Internet und auf dem zweiten Abschnitt im *PSTN* statt. Die Übermittlung erfordere deshalb den Abschluss von Vereinbarungen zwischen Skype Communications und den Telekommunikationsdienstleistern.[38] Daraus ergebe sich, dass die *SkypeOut*-Funktion überwiegend darin bestehe, die Sprachsignale über die elektronischen Kommunikationsnetze, nämlich zunächst das Internet, dann das *PSTN*, von anrufenden NutzerInnen an angerufene NutzerInnen zu übertragen.[39] Es sei somit davon auszugehen, dass Skype Communications gegenüber den NutzerInnen der *SkypeOut*-Funktion, die diesen Dienst bezahlen, für die Übermittlung der Sprachsignale über das *PSTN* die Verantwortung übernehme.[40]

Den entscheidenden Unterschied zwischen *SkypeOut* und *Gmail* stellt in den Ausführungen des EuGH demnach die Verantwortlichkeit für die Signalübertragung dar. Während *Gmail* die Möglichkeit der Signalübertragung einfach voraussetzt, ist *SkypeOut* dazu gezwungen, die Zustellung der Telefonate zu den EmpfängerInnen selbst zu gewährleisten, weshalb *SkypeOut* die Verantwortung für die Übertragung der Signale zugerechnet werden kann. Festzuhalten bleibt, dass *OTT*-Kommunikationsdienste somit grundsätzlich nicht der sektorspezifischen Regulie-

rung unterfallen, weshalb sie weder der Meldepflicht nachkommen müssen, noch durch die telekommunikationsrechtlichen Vorschriften über Datenschutz und die öffentliche Sicherheit verpflichtet sind.[41] Dabei ist für die Klassifizierung eines *OTT*-Kommunikationsdienstes das Kriterium der Verantwortlichkeit entscheidend. Ist einem Dienst die Verantwortung für die Übermittlung der Signale über die Fest- oder Mobilfunknetze (etwa ab der Gateway-Verbindung) zurechenbar, so sind die telekommunikationsrechtlichen Vorschriften dennoch anwendbar.[42]

Bundesverfassungsgericht zu *Posteo*

Es ist davon auszugehen, dass die Auslegung der Verantwortlichkeit im Rahmen der *Gmail*-Entscheidung auf einen großen Teil der *OTT*-Kommunikationsdienste übertragbar sein dürfte, unabhängig davon, ob es sich dabei um *Client-Server*-Modelle oder *Peer-to-Peer*-Modelle handelt.[43]

Dies betrifft auch den E-Mail-Dienst *Posteo*, der dazu aufgefordert wurde, die für eine Telekommunikationsüberwachung benötigte Infrastruktur vorzuhalten.[44] Die Verfassungsbeschwerde des Dienstes wurde jedoch nicht vom Bundesverfassungsgericht (BVerfG) angenommen. In seinem Nichtannahmebeschluss vom 20.12.2018 bestätigte das BVerfG die Auffassung, dass *Posteo* gem. § 110 Abs. 1 S. 1 Nr. 1 TKG in Verbindung mit § 3, § 5 Abs. 1 und 2, § 6 Abs. 1 sowie § 7 Abs. 1 S. 1 Nr. 4 der Telekommunikations-Überwachungsverordnung (TKÜV) verpflichtet ist, seinen Betrieb so zu gestalten, dass bei dem Unternehmen vorhandene IP-Adressen für Maßnahmen der Telekommunikationsüberwachung bereitgestellt werden müssen.[45] *Posteo* wird somit telekommunikationsrechtlich reguliert. Ob es sich bei *Posteo* jedoch überhaupt um einen Kommunikationsdienst handelt, hinterfragt das BVerfG in seiner Entscheidung nicht. Es legt lediglich einen »›weiten‹ Telekommunikationsbegriff«[46] gem. § 3 Nr. 22 TKG zugrunde, wonach Telekommunikation »der technische Vorgang des Aussendens, Übermittelns und Empfangens von Signalen mittels Telekommunikationsanlagen« ist. Demnach unterliege laut den Ausführungen des BVerfG auch der Zugriff auf E-Mail-Kommunikation unstrittig dem Anwendungsbereich der Telekommunikationsüberwachung gem. § 100a der Strafprozessordnung (StPO).[47] Das BVerfG geht somit davon aus, dass es sich bei *Posteo* um einen »[...] Betreiber einer Telekommunikationsanlage [...]«[48] handelt. § 110 Abs. 1 S. 1 Nr. 1 TKG verpflichtet dabei die Dienstanbieter als Betreiber von Telekommunikationsanlagen, mit denen öffentliche Telekommunikationsdienste erbracht werden, Maßnahmen zur Überwachung der Telekommunikation vorzuhalten.[49]

In Anbetracht der *Gmail*-Entscheidung des EuGH ist jedoch davon auszugehen, dass auch *Posteo* nicht länger als Betreiber einer Kommunikationsanlage, mit der öffentliche Kommunikationsdienste erbracht werden, eingestuft werden kann. Einziges signifikantes Unterscheidungsmerkmal, welches gegebenenfalls eine verschiedenartige Behandlung beider Dienste begründen könnte, sind die unterschiedlichen Formen der Finanzierung der jeweiligen Geschäftsmodelle. Während *Posteo*, ähnlich wie *SykpeOut*, eine monatliche Gebühr von den NutzerInnen verlangt,[50] finanziert sich *Gmail* durch Werbung und ggf. durch andere indirekte Einnahmen. Wie bereits erwähnt, lässt der EuGH im Rahmen der *Gmail*-Entscheidung die dritte Frage in Bezug auf die Entgeltlichkeit von Diensten offen, jedoch geht das VG Köln in seiner Entscheidung aus dem Jahr 2015 von einer Gewerblichkeit *Gmail*s aus, da es nicht notwendig sei, dass die Gegenleistung auch vom Empfänger der Leistung erbracht werden müsse.[51] Im Falle einer Werbefinanzierung erbringe der Werbende und nicht die NutzerInnen die Gegenleistung, sodass der Dienst als entgeltpflichtig anzusehen sei.[52] Eine Ungleichbehandlung beider E-Mail-Dienste erscheint somit nicht gerechtfertigt, zumal darüber hinaus keine Unterschiede beim ausschlaggebenden Kriterium der Verantwortlichkeit in Bezug auf die ganz oder überwiegende Signalübertragung erkennbar sind. Es kann demnach angenommen werden, dass auch der E-Mail-Dienst *Posteo,* ebenso wie *Gmail,* nicht den sektorspezifischen telekommunikationsrechtlichen Regelungen unterfällt und somit nicht gem. § 110 Abs. 1 S. 1 Nr. 1 TKG als Betreiber einer Telekommunikationsanlage verpflichtet werden kann.

Umfassender Regelungsrahmen für *OTT*-Dienste – auch in Zukunft?

Schlussendlich bleibt festzuhalten, dass durch die *Gmail*-Entscheidung eine trennschärfere Abgrenzung von elektronischen Kommunikationsdiensten und *OTT*-Diensten ermöglicht worden ist. Die für die Einordnung eines Dienstes entscheidende Frage der ganz oder überwiegenden Signalübertragung wird dabei vom Kriterium der Verantwortlichkeit abhängig gemacht.[53] In Zusammenschau mit dem *SkypeOut*-Urteil wird dabei zugleich eine weitgehend stimmige Einordnung von hybriden Formen der *OTT*-Kommunikation gewährleistet.[54]

Reine *OTT*-Kommunikationsdienste unterliegen in Folge des *Gmail*-Urteils nicht den bereichsspezifischen telekommunikationsrechtlichen Vorschriften. *Gmail*, *Posteo*, *WhatsApp*, *Telegram* und vergleichbare Anbieter müssen deshalb weder der Meldepflicht nachkommen noch sind die telekommunikationsrechtlichen Vorschriften über Datenschutz und die

öffentliche Sicherheit auf diese anwendbar.[55] Insgesamt ist das *Gmail*-Urteil jedoch eher als »zeitlich begrenzter Sieg«[56] für die *OTT*-Anbieter zu werten, da sich die Rechtslage bereits in naher Zukunft ändern wird. Im Dezember 2018 ist die Richtlinie 2018/1972 über den europäischen Kodex für die elektronische Kommunikation (EKEK) verabschiedet worden, die bis zum 21.12.2020 von den Mitgliedstaaten umzusetzen ist. Gem. Art. 2 Nr. 4 lit. b EKEK sind von den elektronischen Kommunikationsdiensten nun auch interpersonelle Kommunikationsdienste umfasst, die gem. Art. 2 Nr. 5 EKEK »einen direkten interpersonellen und interaktiven Informationsaustausch über elektronische Kommunikationsnetze zwischen einer endlichen Zahl von Personen ermöglichen, wobei die Empfänger von den Personen bestimmt werden, die die Kommunikation veranlassen oder daran beteiligt sind«. Diese Definition erfasst somit auch *OTT*-Kommunikationsdienste; auf die bisher entscheidende Frage der ganz oder überwiegenden Signalübertragung wird es demnach zukünftig nicht mehr ankommen.

Nichtsdestotrotz werden nummerngebundene interpersonelle Kommunikationsdienste, wie etwa *Skype-Out,* auch künftig stärker reguliert als nummernunabhängige Dienste,[57] da gem. ErwG 18 EKEK nummerngebundene Dienste »am öffentlich gesicherten interoperablen Ökosystem beteiligt sind und somit auch Nutzen daraus ziehen.« »Nummernunabhängige interpersonelle Kommunikationsdienste sollen [jedoch] nur dann Verpflichtungen unterliegen, wenn das öffentliche Interesse erfordert, dass spezifische regulatorische Verpflichtungen auf alle Arten von interpersonellen Kommunikationsdiensten Anwendung finden.« In Bezug auf die Meldepflicht wird sich dennoch auch mit Umsetzung des EKEK nichts ändern, da dieser gem. Art. 12 EKEK nur nummerngebundene nicht aber auch nummernunabhängige interpersonelle Kommunikationsdienste, wie etwa *Gmail*, nachkommen müssen.[58] Für die Anwendung der Vorschriften der EKEK über die Sicherheit von Netzen und Diensten ist hingegen nicht von Bedeutung, ob es sich um einen nummernunabhängigen oder nummerngebundenen interpersonellen Kommunikationsdienst handelt.[59] Zuletzt wird auch die vom EuGH offengelassene dritte Frage des OVG Münster in Bezug auf die Entgeltlichkeit von Diensten durch ErwG 16 EKEK geklärt: So werden in Zukunft auch Fälle erfasst, in denen EndnutzerInnen als Bedingung für den Zugang zu dem Dienst Werbung ausgesetzt sind oder vom Dienst erhobene personenbezogene Daten kommerziell verwertet werden.[60]

Patrick Herget

Wissenschaftlicher Mitarbeiter am DFG-Graduiertenkolleg »Privatheit und Digitalisierung«.

Endnoten

1 Vgl. EuGH: *Urt. v. 13.06.2019, Rs. C-193/18 – Gmail.* ECLI:EU:C:2019:498, Rn. 41. Im Folgenden zitiert als EuGH 13.06.2019, juris.
2 Vgl. Ludwigs, Markus/Huller, Felix: OTT-Kommunikation: (Noch) Keine TK-Regulierung für Gmail & Co.. In: *NVwZ.* Nr. 15, 2019, S. 1099–1101, hier S. 1099.
3 Vgl. Anmerkungen des OVG NRW im Vorlagebeschluss: OVG NRW: *Vorlagebeschl. v. 26.02.2018 – 13 A 17/16.* EC LI:DE:OVGNRW:2018:0226.13A17.16.00. Im Folgenden zitiert als OVG NRW 26.02.2018, juris.
4 Gremium Europäischer Regulierungsstellen für elektronische Kommunikation: Draft Report on OTT Services. In: *BoR* (16) 35, 2016, S. 14. Online: https://berec.europa.eu/eng/document_register/subject_matter/berec/reports/5751-berec-report-on-ott-services (02.09.2019).
5 Vgl. Grünwald, Andreas/Nüßing, Christoph: Kommunikation over the Top – Regulierung für Skype, WhatsApp oder Gmail?. In: *MMR.* Nr. 2, 2016, S. 91–97, hier S. 92.
6 Vgl. Grünwald/Nüßing 2016, S. 92.
7 Vgl. dazu: Grünwald/Nüßing 2016, S. 92 f.
8 Vgl. Ludwigs/Huller 2019, S. 1099.
9 Vgl. Hoeren, Thomas: Bitte melden bei der Bundesnetzagentur. In: *Legal Tribune Online* vom 12.06.2019. Online: https://www.lto.de/recht/hintergruende/h/eugh-c-193-18-gmail-internetdienste-bundesnetzagentur-telekommunikationsgesetz/ (10.08.2019).
10 EuGH: *Urt. v. 05.06.2019, Rs. C-142/18 – Skype Communications.* ECLI:EU:C:2019:460. Im Folgenden zitiert als EuGH 05.06.2019, juris.
11 Vgl. EuGH 13.06.2019, juris, Rn. 14 f.
12 Vgl. VG Köln: *Urt. v. 11.11.2015 – 21 K 450/15.* ECLI:DE:VGK:2015:1111.21K450.15.00, Rn. 45. Im Folgenden

zitiert als VG Köln 11.11.2015, juris.
13 Vgl. VG Köln 11.11.2015, juris, Rn. 47.
14 VG Köln 11.11.2015, juris, Rn. 57.
15 VG Köln 11.11.2015, juris, Rn. 59.
16 Vgl. VG Köln 11.11.2015, juris, Rn. 59.
17 Vgl. VG Köln 11.11.2015, juris, Rn. 51.
18 Vgl. OVG NRW 26.02.2018, Rn. 5.
19 Vgl. EuGH 13.06.2019, juris, Rn. 21.
20 Bei einem »Best-Effort«-Dienst vergibt das Protokoll keine Garantien und keine Prioritäten, die zu sendenden Pakete werden einfach nach bestem Bemühen verschickt (Prinzip: »Man tut was man kann!«). Vgl. dazu: Uni Hamburg: *»best-effort«-Dienst* 2019. Online: http://www.informatik.uni-hamburg.de/TKRN/world/lernmodule/LMvk/Popup/besteffort.html (04.09.2019).
21 Vgl. EuGH 13.06.2019, juris, Rn. 21.
22 Vgl. EuGH 13.06.2019, juris, Rn. 21.
23 EuGH 13.06.2019, juris, Rn. 25.
24 Vgl. EuGH 13.06.2019, juris, Rn. 34.
25 Vgl. EuGH 13.06.2019, juris, Rn. 35.
26 Vgl. EuGH: *Urt. v. 30.04.2014, Rs. C-475/12 – UPC DTH.* ECLI:EU:C:2014:285, Rn. 43.
27 Vgl. EuGH 13.06.2019, juris, Rn. 36.
28 Vgl. EuGH 13.06.2019, juris, Rn. 37.
29 Vgl. EuGH 13.06.2019, juris, Rn. 38, 42.
30 Vgl. EuGH 13.06.2019, juris, Rn. 39.
31 Vgl. EuGH 13.06.2019, juris, Rn. 42.
32 Hoeren 2019.
33 Vgl. ebd.
34 Vgl. Muth, Max: Gmail gilt nicht als elektronischer Kommunikationsdienst. In: *Sueddeutsche.de* vom 13.06.2019. Online: https://www.sueddeutsche.de/digital/google-e-mail-eugh-bundesnetzagentur-1.4484955 (09.08.2019).
35 Vgl. EuGH 05.06.2019, juris, Rn. 12.
36 Vgl. Skype: Erfahren Sie, wie günstig Anrufe ins In- und Ausland mit den Tarifen von Skype für Auslandsanrufe sind 2019. Online: https://www.skype.com/de/international-calls/ (01.09.2019).
37 Vgl. EuGH 05.06.2019, juris, Rn. 30.
38 Vgl. EuGH 05.06.2019, juris, Rn. 34 f.
39 Vgl. EuGH 05.06.2019, juris, Rn. 33.
40 Vgl. ebd.
41 Vgl. Ludwigs/Huller 2019, S. 1101.
42 So auch: Ludwigs/Huller 2019, S. 1101.
43 Vgl. Ludwigs/Huller 2019, S. 1099.
44 Siehe dazu die detaillierten Ausführungen von Felix Sobala und Lea Watzinger in diesem Heft.
45 Vgl. BVerfG: *Beschl. v. 20.12.2018 – 2 BvR 2377/16.* ECLI:DE:BVerfG:2018:rk20181220.2bvr237716, Rn. 41. Im Folgenden zitiert als BVerfG 20.12.2018, juris.
46 BVerfG 20.12.2018, juris, Rn. 42.
47 Vgl. ebd.
48 BVerfG 20.12.2018, juris, Rn. 45.
49 Vgl. BVerfG 20.12.2018, juris, Rn. 46.
50 Vgl. Posteo: Ihr Postfach: *Nachhaltig, sicher und werbefrei* 2019. Online: https://posteo.de/site/leistungen (01.09.2019).
51 Vgl. VG Köln 11.11.2015, juris, Rn. 47.
52 Vgl. VG Köln 11.11.2015, juris, Rn. 45.
53 Vgl. EuGH 13.06.2019, juris, Rn. 32.
54 Vgl. Ludwigs/Huller 2019, S. 1099 f.
55 Vgl. Ludwigs/Huller 2019, S. 1101.
56 Legal Tribune Online: Ein zeitlich begrenzter Sieg für Gmail 2019. Online: https://www.lto.de/recht/nachrichten/n/eugh-c-193-18-gmail-google-bundesnetzagentur-telekommunikation/ (01.09.2019).
57 Vgl. Ludwigs/Huller 2019, S. 1101.
58 Vgl. ebd.
59 Vgl. ebd.
60 Vgl. ebd.

Operation »Autowäsche«: vom Ruhm zum Zweifel

Privatheit und Informationsfreiheit in Brasiliens größtem Korruptionsskandal

Foto: REUTERS / NACHO DOCE - stock.adobe.com

von Gustavo Gil Gasiola

The Carwash Operation (2014–2019), being one of the largest investigations into corruption in Brazil, brought about radical political changes, from the impeachment of President Rousseff to the election of a far-right candidate as president. That the Operation had a specific background became evident when the website *The Intercept Brazil* published a *Telegram*'s data leak that included private e-correspondence between judges and federal prosecutors. On the one hand, the violation of the right of privacy here was evident. On the other hand, however, citizens have the right to access the information, which is of public interest. This contribution analyses the correlation between the protection of privacy and the right of access to the information of public relevance on the example of the Carwash scandal in Brazil.

HISTORIE

2014
»Operation Autowäsche« beginnt. Ermittlung des größten Korruptionsskandals Brasiliens.

2016
Amtsenthebungsverfahren im Fall der Präsidentin Dilma Rousseff. Der Vize-Präsident Michel Temer übernimmt die Regierung.

2017
Richter Sergio Moro verurteilt wegen Korruption den früheren Präsidenten Luis Inácio Lula da Silva.

2018
Inhaftierung des Präsidenten Lula da Silva: Er kann nicht an der Präsidentschaftswahl 2018 teilnehmen.
Der ultrarechte Jair Bolsonaro wird gewählt und Sergio Moro als Justizminister nominiert.

2019
Die Internetplattform »The Intercept Brazil« veröffentlicht private Kurznachrichten von Sergio Moro und den Staatsanwälten der Operation Autowäsche und stellt die Unparteilichkeit des Urteils in Frage.

Im Juni 2019 veröffentlichte die Internetplattform »The Intercept Brazil« *Telegram*-Kurznachrichten einzelner Richter und Staatsanwälte, die an den Prozessen zu einem der größten Korruptionsskandale Brasiliens beteiligt waren. Trotz Verletzung der Privatsphäre deckte das Daten-Leak eine rechtswidrige Beziehung zwischen den Autoritäten auf. Folglich sind die durchgeführten Ermittlungen als politisch motiviert und parteiisch einzustufen. Vor diesem Hintergrund widmet sich der folgende Beitrag der juristischen Einordnung des Verhältnisses zwischen dem Schutz der Privatsphäre und dem öffentlichen Informationsinteresse nach brasilianischem Recht am Beispiel des Daten-Leaks der »Operation Autowäsche«.

Baufirmen im Visier

2014 begann in Brasilien die Polizei-Operation *Lava Jato* (»Autowäsche«). Von einer relativ kleinen Ermittlung über Geldwäsche deckte die Bundespolizei zusammen mit der Staatsanwaltschaft (*Ministério Público Federal*) den größten Korruptionsskandal der brasilianischen Geschichte auf.[1] Das Ziel der Ermittlungen waren Baukonzerne und politische Eliten, wobei im Laufe der Ermittlungen viele Personen des öffentlichen Lebens inhaftiert wurden, wie etwa der frühere Landeschef von Rio de Janeiro oder der Präsident von Odebrecht, des größten Baukonzerns Brasiliens. Die Operation erhielt in der Öffentlichkeit viel Aufmerksamkeit und machte zusätzlich ein wenig Hoffnung, dass die chronischen Korruptionsprobleme Brasiliens vielleicht lösbar wären. Der für die Ermittlungen zuständige Richter, Sergio Moro, wurde zum Helden und dadurch zum Gesicht der ganzen Operation erklärt.

Dabei spielten die Ermittlungen im politischen Diskurs eine immer größere Rolle und verstärkten die existierende Polarisierung der Gesellschaft. Deckte die Untersuchung PolitikerInnen oder eine Partei auf, wurden diese schnell als Schuldige aller brasilianischen Probleme dargestellt. Je größer die Ermittlung wurde, umso stärker wurde die Politik an sich dämonisiert, mit der Folge, dass es auf den Straßen zu Demonstrationen von Unterstützern für die Operation Lava Jato und Richter Moro kam, auf denen wahlweise die Rückkehr der Diktatur oder der Monarchie gefordert wurde. Teile der Opposition schafften es außerdem, diesen Missmut in eine Trennung von ›alter‹ und ›neuer‹ Politik zu übersetzen und davon zu profitieren.

Die Oppositionsparteien nutzen Korruptionsskandale regelmäßig als Instrument, um politischen Druck auszuüben und Regierungen, PräsidentInnen oder Parteien zum Rücktritt oder zu Neuwahlen zu zwingen. Das gehört zur Demokratie. Was aber nicht dazu gehört, ist die politische Nutzung der Justiz. RichterInnen müssen unparteiisch sein.[2] Die Recht sprechende Gewalt muss eine klare Trennung

zwischen politischer und rechtlicher Ebene gewährleisten. Trotzdem wurde mit Beginn der Operation die Unparteilichkeit von Sergio Moro in Frage gestellt.[3]

In den letzten Jahren gab es einen grundlegenden Wandel der politischen Landschaft in Brasilien, auch aufgrund der »Operation Autowäsche«. Zweifellos hatte die Operation einen großen Anteil am Amtsenthebungsverfahren 2016 der früheren Präsidentin Dilma Rousseff (2011-2016) sowie der Präsidentschaftswahl 2018, bei der der ultrarechte Jair Bolsonaro gewählt wurde. Auf der einen Seite war Rousseff selbst von keinem Korruptionsskandal betroffen, aber ihre Partei (die linke Arbeiterpartei PT – *Partido dos Trabalhadores*) war das Hauptziel der Operation, was ausreichte, um ihre Glaubwürdigkeit anzuzweifeln.

Auf der anderen Seite stellte Bolsonaro die ›neue‹ Politik dar. Das wurde möglich, weil er nicht selbst von der Operation betroffen war. Darüber hinaus konnte der klare Favorit der Präsidentchaftswahl 2018, das Arbeiterparteimitglied und der frühere Präsident Lula da Silva (2003-2010), an der Wahl nicht teilnehmen, da er im Januar 2018 wegen Korruption verurteilt wurde. Die Tatsache, dass es in dem Prozess Lulas keine Beweise gab und die Korruption nur anhand von Indizien und Zeugenaussagen, die nach brasilianischem Recht als keine/nicht ausreichende Beweismittel betrachtet werden dürfen, bewiesen wurde, wurde von einer Vielzahl von JuristInnen kritisiert.[4]

Kurz nach der Präsidentschaftswahl 2018 nominierte Bolsonaro Richter Moro als Justizminister. Während UnterstützerInnen Bolsonaros die Nominierung begrüßten und als weiteren Schritt im Kampf gegen die Korruption sahen, verstärkte sich auf der politischen Gegenseite der Verdacht der Parteilichkeit der Operation *Lava Jato*. Hatte der frühere Richter Moro die politische Ebene beeinflussen wollen? Auf diese Frage gab es bisher keine Antwort, da alle Argumente gegen Moro mit dem Mantel seiner richterlichen Funktion verweigert werden konnten. Ob die Ermittlung politische Ziele hatte, war nur bloße Vermutung. Scheinbar hatte der Richter einfach seine Funktion erfüllt.

Telegram-Leaks

Der ehemalige Richter und aktuelle Justizminister sah Anfang Juni 2019 die erste Bedrohung gegen sein scheinbares Antikorruptionsvermächtnis. Durch eine anonyme Quelle erhielt die Internetplattform »The Intercept Brazil« eine Reihe von privaten Kurznachrichten, Fotos, Tonaufnahmen und anderen Dateien, die im Kurznachrichtendienst *Telegram* gespeichert worden waren.[5] Die Daten bezogen sich auf die Kommunikation zwischen den Akteuren der Operation »Autowäsche«, einschließlich Richter Moro und Staatsanwälten und enthüllten deren Beziehungen und Tätigkeiten im Hintergrund der Operation.

Laut dieser Nachrichten war Moro ein parteiischer Richter. Die StaatsanwältInnen bekamen von ihm Vorschläge zu Zeugen und Beweisen. Demnach traf sich Moro regelmäßig mit der Polizei und der Staatsanwaltschaft, um die Operation zu planen. Obwohl die Polizei unabhängig ist, empfahl Moro einen anderen Termin zu einer geheimen Durchsuchung und Beschlagnahmung. Außerdem tadelte er die Ermittlung gegen den früheren Präsident Fernando Henrique Cardoso (1995-2002), weil er ein »Alliierter« wäre. Zusammenfassend arbeitete der Richter zusammen mit dem Ankläger zum Nachteil der Angeklagten. Beide, Moro und StaatsanwältInnen, sahen die Arbeiterpartei und insbesondere Lula als politische Gegenseite.

Diese politische Motivation bestätigt aber einfach, dass Moro die Stelle als Justizminister als ›Preis‹ für das Wahlergebnis bekam. Bolsonaro war der Kandidat der Operation »Autowäsche«. Während des Wahlkampfes hatten Moro und Staatsanwälte per *Telegran* Strategien gegen die Arbeiterpartei überlegt. Sie waren eindeutig beunruhigt.

Moro verneint zwar alle Vorwürfe, aber seine Verteidigung ist nicht glaubhaft. Zuerst hatte Moro behauptet, dass die Daten durch einen Hackeranschlag gestohlen wurden. Danach stellte er die Authentizität der Nachrichten in Frage. Dann sagte er aber, auch wenn die Nachrichten unverfälscht seien, würden ihre Inhalte nichts Rechtswidriges zeigen. Schließlich warf Moro den Zeitungen vor, dass diese Zeitungen alle korrupten Politiker befreien wollten.

Privatheit und Informationsfreiheit

Die Veröffentlichung von privaten Nachrichten entspricht einem klaren Konflikt zwischen Rechtsgütern. Die Privatheit und auch die Geheimhaltung des privaten Kommunikationsmittels[6] und privaten Lebens[7] stehen in dem Fall der Informationsfreiheit[8] gegenüber. Als Richter übte Moro zwar eine öffentliche Stelle aus, dies schließt den Schutz gegen Eingriffe auf seine private Kommunikation aber nicht aus. Alle Menschen werden in ihrer eigenen Meinung, ihren sozialen Kontakten und anderen Beziehungen durch die Menschenwürde und das Persönlichkeitsrecht verfassungsrechtlich geschützt.[9] Außerdem verbietet die behördliche Funktion RichterInnen und StaatsanwältInnen nicht, Freunde zu haben und miteinander zu kommunizieren.

Trotzdem gewährleistet die Verfassung auch die Informationsfreiheit.[10] Medien besitzen diese Freiheit als eine Voraussetzung ihrer Tätigkeiten. Hinzufügend

müssen Zeitungen die Identität ihrer Quellen nicht offenbaren, denn die Anonymität ist auch verfassungsrechtlich geschützt.[11] Und dies gilt auch, wenn die Quelle ein Straftäter (z. B. Hacker) ist.

Eine Abwägung zwischen beiden Interessen (Privatheit und Informationsfreiheit) ist deswegen erforderlich. Auf der einen Seite gewährleistet Privatheit die freie Entfaltung der Persönlichkeit. Diese verweigert den ungewünschten Zugang Dritter zu privaten Angelegenheiten. Dieser Schutz ist aber kein Instrument, um abseits der Öffentlichkeit illegalen Tätigkeiten nachzugehen. Mit angemessenen Gründen und in Einklang mit dem Gesetz ist der Einblick in der Privatsphäre erlaubt. Dies gilt insbesondere bei der Offenlegung von Rechtswidrigkeiten.

Auf der anderen Seite gewährleistet Informationsfreiheit wiederum, dass die gesellschaftlich relevanten Informationen verbreitet werden. Dieses Grundrecht gibt der Presse zusammen mit dem Transparenzprinzip der öffentlichen Verwaltung[12] eine aktive Rolle. JournalistInnen können damit die öffentlichen Tätigkeiten überwachen. Für die Bevölkerung sind die Informationsfreiheit und die Rolle der Presse eine Voraussetzung der Demokratie. Alle haben das Recht zu wissen, wenn sich Beamte rechtswidrig verhalten.

Freundschaft und Unparteilichkeit

Die private Beziehung zwischen RichterInnen und Beteiligten eines Prozesses ist zulässig. Sie dürfen miteinander kommunizieren, soweit sich ihre Beziehung auf eine einfache Freundschaft beschränkt. Nach brasilianischer Rechtsprechung widerspricht jedoch eine enge Freundschaft zwischen RichterInnen und Beteiligten der Unparteilichkeit. Eine solche Differenzierung ist allerdings schwierig und im Einzelfall eher schwer zu treffen. Während der Verwandtschaftsgrad enge Freundschaft voraussetzt,[13] wird die ausschließliche Verbindung auf Sozialen Netzwerken als einfache Freundschaft angesehen.[14]

Jedenfalls ist der Verdacht einer rechtswidrigen Beziehung (also einer engen Freundschaft) ohne weiteres Indiz kein ausreichender Grund, in die Privatsphäre von irgendjemand einzudringen. Der vorsorgliche Zugang zu einem privaten Kommunikationsmittel ist zweifellos eine unangemessene Verletzung des Grundsatzes des Persönlichkeitsrechts. Sobald es einen ausreichenden Grund (z.B. Ermittlung einer Straftat gegen wichtige Rechtsgüter) gibt, gilt aber eine solche Abweichung als gerechtfertigt.

Die Behauptung, dass Moro mit den StaatsanwältInnen zusammengearbeitet habe, rechtfertigte aber keine Offenbarung des privaten Lebens des Beamten. Ob ein Komplott gegen Lula stattgefunden hatte, durfte nicht auf Kosten der Privatheit des Richters untersucht werden.

Aus diesem Grund ist die Veröffentlichung des *Telegram*-Leaks zweifellos rechtswidrig. Wenn die TäterInnen ermittelt werden, werden sie strafrechtlich verurteilt. Anders stellt sich die Situation für die Internetplattform »The Intercept Brazil« dar, deren Tätigkeit durch die Informationsfreiheit geschützt ist. Ihr Bericht ist nicht von der Rechtmäßigkeit der Quelle abhängig, d. h., die eventuelle Rechtswidrigkeit der Datensammlung beeinträchtigt die gesellschaftliche Relevanz der Informationen nicht. Die Veröffentlichung darf deswegen nicht beschränkt werden, da dies Zensur wäre.

Obwohl die Quelle strafrechtlich verantwortlich ist, ist es die Zeitung nicht (es sei denn, MitarbeiterInnen der Zeitung wären gleichzeitig auch die TäterInnen). Es gibt eine klare Trennung zwischen der Straftat und den journalistischen Tätigkeiten. Solange diese getrennt sind, bleibt auch die Strafbarkeit getrennt. Selbstverständlich verletzt die Veröffentlichung privater Kurznachrichten das Persönlichkeitsrecht. Der Daten-Leak lässt sich mit einem Eindringen in die Privatsphäre des Richters gleichsetzen. Deswegen hat die Informationsfreiheit auch Beschränkungen. Nach sorgfältiger Abwägung darf die Zeitung alles veröffentlichen, soweit die Informationen von gesellschaftlicher Relevanz sind.[15] Wenn Moro eine Affäre hätte, wäre es fragwürdig, ob ein Eingriff in die Privatheit des Richters gerechtfertigt wäre. Beginge Moro jedoch eine relevante Straftat, ist nun das öffentliche Interesse der Veröffentlichung klar zu identifizieren. Trotz der Informationsfreiheit muss die Zeitung den Bericht selektiv veröffentlichen. Was rein private Angelegenheiten des Richters sind, darf nicht veröffentlicht werden.

Die Nachrichten von *The Intercept Brazil* sind bisher gesetzeskonform. Sie berichten von einer rechtswidrigen Beziehung zwischen Moro und den Staatsanwälten. Die Beamten benutzten *Telegram*, um sich bei der Operation »Autowäsche« abzusprechen. Der private Raum wurde inoffiziell als Verlängerung der staatlichen Funktionen (jeweils Richter und Ankläger) genutzt. Da die Kurznachrichten die Unparteilichkeit der Operation in Frage stellen, entspricht die Berichterstattung darüber dem öffentlichen Interesse.

Fazit

Das *Telegram*-Leak hatte und hat noch wichtige Folgen. Große Zeitungen, JournalistInnen und JuristInnen stehen der Operation »Autowäsche« mittlerweile kritisch gegenüber. In der Bevölkerung ist bereits ein steigendes Misstrauen bemerkbar, seit die Demonstrationen für Moro immer kleiner

werden. Keinesfalls wurde die politische Polarisierung aufgelöst. Für die Opposition (Linksparteien) waren die Operation und ihre Akteure immer politisch motiviert. Die Regierung und ihre UnterstützerInnen behaupten demgegenüber, dass alle Vorwürfe gegen die Operation »Autowäsche« ein Bestreben zeige, die Korruptionsbekämpfung zu behindern.

Rechtlich sind die Folgen des *Telegram*-Leaks noch unklar. Die geleakten und veröffentlichten Kurznachrichten dürfen als Beweis gegen die Staatsanwälte und Moro nicht benutzt werden, da sie illegal beschafft wurden.[16] Dadurch können die verdächtigten Beamten durch den Inhalt der Kurznachrichten nicht verantwortlich gemacht werden. Unabhängig davon dürfen rechtswidrige erlangte Beweismittel nach Rechtsprechung des brasilianischen Bundesverfassungsgerichts[17] verwertet werden, wenn sie eine Strafverfolgung der Beklagten begünstigen. Zumindest in dem Fall Lula ist schon festzustellen, dass Moro parteiisch handelte und deswegen im Prozess gegen Lula nicht persönlich das Urteil sprechen durfte. Dies bedeutet aber nicht, dass Lula unschuldig wäre.

In den kommenden Monaten werden die Kurznachrichten vor dem brasilianischen Bundesverfassungsgericht analysiert. Ihre Authentizität wird nachgeprüft und ihr Inhalt eingeschätzt. Gilt die Parteilichkeit von Richter Moro als erwiesen, muss dann die erstinstanzliche Entscheidung aufgehoben werden. Darüber hinaus würde die zweitinstanzliche Entscheidung damit ebenfalls aufgehoben, mit bisher noch nicht absehbaren Folgen.

Gustavo Gil Gasiola

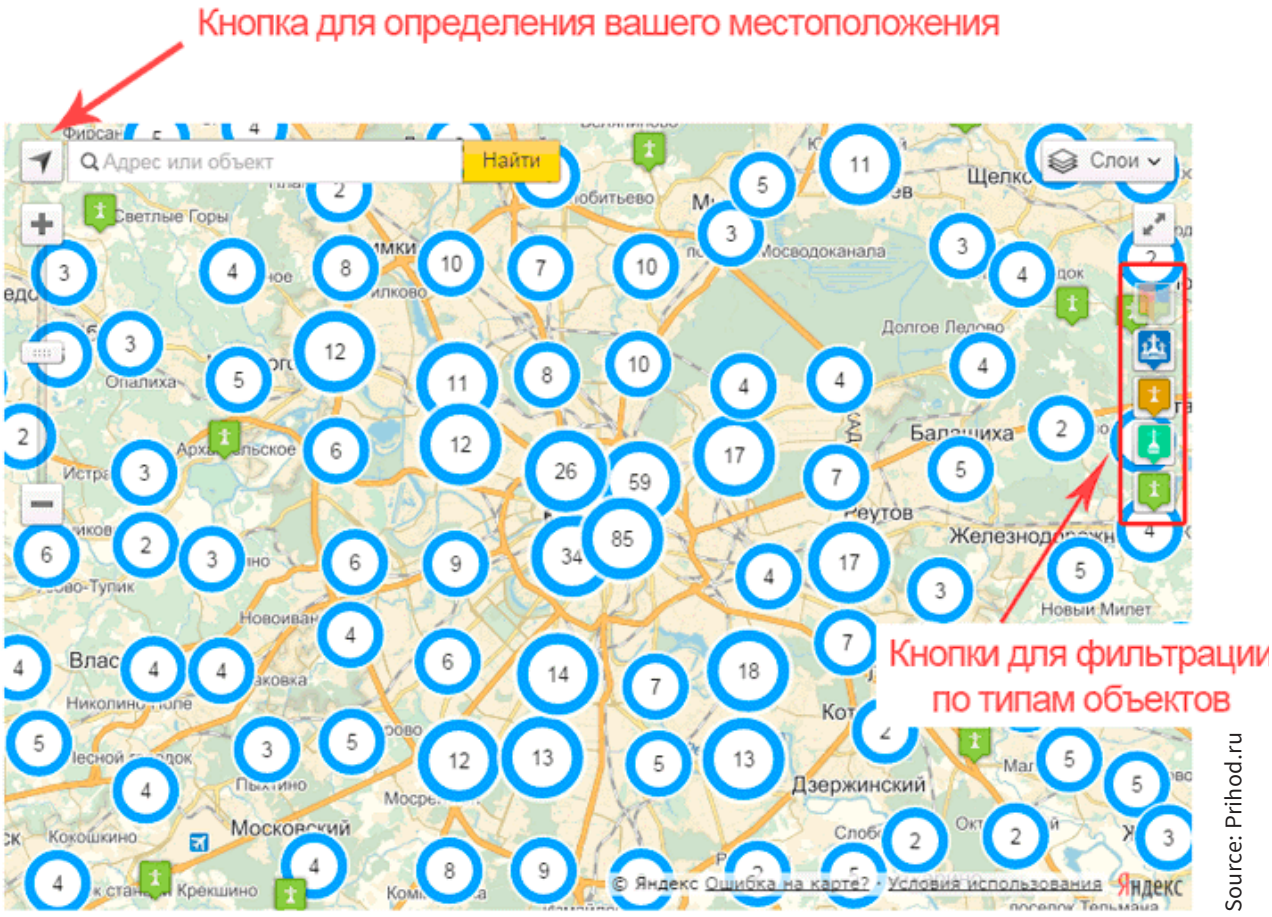
DAAD-Stipendiat am DFG-Graduiertenkolleg »Privatheit und Digitalisierung«.

Endnoten

1 Siehe Ministério Público Federal: Caso Lava Jato. Online: http://www.mpf.mp.br/grandes-casos/lava-jato/entenda-o-caso (11.11.2019).
2 Constituição da República Federativa do Brasil de 1988 (brasilianische Verfassung), § 5º, XXXVII und LIII.
3 Vgl. Costa, Petra: *Democracia em Vertigem* (»Am Rande der Demokratie«), Netflix, 2019.
4 Vgl. Comunidade jurídica debate argumentos do jugamento do ex-presidente Lula: *Conjur* 2018. Online: https://www.conjur.com.br/2018-jan-24/comunidade-juridica-debate-argumentos-julgamento-lula (11.11.2019).
5 Greenwald, Glenn/Reed, Betsy/Demori, Leandro: Como e por que o Intercept está publicando chats privados sobre a Lava Jato e Sergio Moro. In: *The Intercept Brazil* vom 09.06.2019. Online: https://theintercept.com/2019/06/09/editorial-chats-telegram-lava-jato-moro/ (11.09.2019).
6 Constituição da República Federativa do Brasil de 1988 (brasilianische Verfassung), § 5º, XII.
7 Constituição da República Federativa do Brasil de 1988 (brasilianische Verfassung), § 5º, X.
8 Constituição da República Federativa do Brasil de 1988 (brasilianische Verfassung), § 5º, XIV.
9 Silva, José Afonso da: *Curso de Direito Constitucional Positivo*. São Paulo: Malheiros 2005, S. 208-210.
10 Constituição da República Federativa do Brasil de 1988 (brasilianische Verfassung), § 5º, XIV.
11 Constituição da República Federativa do Brasil de 1988 (brasilianische Verfassung), § 5º, XIV.
12 Constituição da República Federativa do Brasil de 1988 (brasilianische Verfassung), § 37.
13 Superior Tribunal de Justiça, Recurso Especial, 916476 / MA.
14 Tribunal de Justiça do Rio Grande do Sul, Exceção de suspeição, 0261276-19.2015.8.21.7000, 30.03.2016.
15 Diese Diskussion bezieht sich auch auf das Problem des Whistleblowings im Investigativjournalismus. Siehe hierzu Sixt, Manuela/Piegsa, Miriam: Das Gerede vom Helden und Verräter oder: Vom Versuch Whistleblower/ing zu verorten. In: *Magazin des DFG-Graduiertenkollegs »Privatheit und Digitalisierung«*, Nr. 7, 2017, S. 4-7.
16 Constituição da República Federativa do Brasil de 1988 (brasilianische Verfassung), § 5º, LVI.
17 Supremo Tribunal Federal, Reclamação Constitucional nº 2.040/DF, Rel. Min. Néri da Silveira, 21.2.2002.

›Digital‹ Canon Law

On the Innovative Digital Dimension of the Concept of Canonical Territory of the Russian Orthodox Church



Source: Prihod.ru

von Alexander Ponomariov

This contribution researches the intersection between the online thematic mapping and the post-Soviet canon law of the Russian Orthodox Church (ROC) known as the concept of canonical territory, according to which, each Orthodox Church has its jurisdiction whose boundaries are normally recognized, yet sometimes violated, by the other churches. By “uploading” its canonical territory, the ROC implements the strategy of giving up its privacy (cf. *Religion ist Privatsache*) in favor of the “effective presence in the media” and seeks additional publicity. Despite being conservative in nature, the canon law herewith gains a new digital dimension in lockstep with digital modernity. Besides, the connection between the offline canonical territory and its online representation is analyzed against the background of the territorial conflict between the Moscow and Ecumenical Patriarchates.

»Die Macht der Karten«: Mapping Russian Orthodoxy in the Digital Era

In 2015, the Russian Orthodox Church (ROC) launched an online mapping project based on technology similar to Google Maps, which aims to "upload" all its canonical territory (i.e., parishes and other church objects) across the globe. In connection with this initiative, Vladimir Legoida, chairman of the ROC's Department for Relations with Society and Media, summarized the current ROC relationship with the Internet as follows. In an introductory statement at the *Prihod.ru* network that maintains the digital maps discussed herein, he concludes that the debates whether a regular Russian Orthodox parish needs its own "private" website are now in the past. Moreover, it no longer suffices for a church unit to "just have" a website: the church should go as public as possible—and so, its web-presence should meet the state-of-the-art standards of design, quality, and functionality. The ROC, therefore, must live in lockstep with digital modernity.

Scholars over the past few years have paid attention to the relationship between Russian Orthodoxy and the digital media, in particular, how this religion instrumentalizes the new media for its purposes.[1] The author of this article has also contributed to the study of "digital Orthodoxy."[2] The present paper continues the said research, focusing on the intersection between digital mapping, which can be categorized as thematic,[3] and the post-Soviet canon law of the ROC known as the concept of canonical territory. Given that maps and mapping have long been understood as instruments of power that create a special connection between cartography and politics[4]—as *Kartenpolitik*[5]—the ROC's mapping project can be seen not only as *Orientierungshilfe*[6] in the digital era but also and above all as theopolitical and geotheological leverage.

The Concept of Canonical Territory of the Russian Orthodox Church

As the largest Local Orthodox Church (LOC) in the world, the Moscow Patriarchate (MP) after the collapse of the Soviet Union (1991) actively promotes the concept of canonical territory. According to the key promoter thereof, *de jure*, this is a recent development in Orthodox canon law; although *de facto*, it "remains the cornerstone of Orthodox ecclesiology" since the ancient times.[7] In particular, each LOC has a certain canonical jurisdiction whose integrity is normally respected, yet sometimes violated, by the other churches. Within these confines, the other LOCs may not intervene by establishing new parishes, or by appointing bishops or priests to the existing church structures. In this regard, the applicable Statute of the ROC (with amendments as of 2017) extends its jurisdiction over the Russian Federation, Ukraine, Belarus, Moldova, Azerbaijan, Kazakhstan, China, Kyrgyzstan, Latvia, Lithuania, Mongolia, Tajikistan, Turkmenistan, Uzbekistan, Estonia, and Japan. In the end, it also adds "the Orthodox Christians living in other countries and voluntarily joining this jurisdiction."[8]

In practice, the latter item implies countries like Germany, France, or the United States, (where there are a few overlapping canonical jurisdictions), since neither Germany nor the U.S. evidence a national Orthodox tradition in their history. The so-called All-Orthodox Council of 2016 pointed out Germany, in particular, as a region of canonical *disorder*: following Resolution 8 of the constitutive I Ecumenical Council (325 C.E.), the ecclesial order requires that there be only one bishop in town, which precludes any overlapping.

On the other hand, some LOCs today coincide with their nation-states and some exceed national borders and connect to diasporas abroad, which fact eventually leads to a few Orthodox bishops in one town belonging to different canonical jurisdictions. The Ecumenical Patriarchate, still viewed by many Orthodox as a kind of Byzantium after Byzantium, puts forth the claim that all the ecclesial space outside the purview of the existing LOCs constitutes its exclusive canonical territory.[9] Based on controversial interpretations of Resolution 28 of the IV Ecumenical Council in Chalcedon (451 C.E.), this claim poses a challenge to the other LOCs, and first and foremost, to the Moscow Patriarchate's presence outside the Russian Federation.[10]

In January 2019, the Ecumenical Patriarchate issued a declaration of independence for the newly created Orthodox Church of Ukraine (OCU), despite the existing canonical Ukrainian Orthodox Church of the Moscow Patriarchate (UOC MP) in the country. This much-debated event has launched a rapid redrawing of ecclesial borders in the Orthodox commonwealth. The conflict is spreading around the globe; and, as a worst-case scenario, it may have "enormous consequences,"[11] because the leaders of the Moscow Patriarchate consider the developments around Ukraine "combat actions" and are ready to fight "to the victorious end."[12]

This church schism stimulates ROC's search for alternative ways to safeguard its territorial integrity. In this context, an appeal to digital *Kartenpolitik* can be seen as an up-to-date instrument to convey the idea of ROC's ecclesial sovereignty to a larger audience.

Canonical Territory on *Facebook*: The Case of North Korea

When the now-famous church council held in Ukraine on 15 December 2018 under the auspices of Constantinople founded the OCU, the ROC already on 28 December 2018 passed a resolution to found a faraway Exarchate of South-Eastern Asia that, thus, would overlap with the canonical jurisdiction of the Ecumenical Patriarchate in the region. In February 2019, the ROC adopted an internal provision on the Exarchate of South-Eastern Asia, which, among other things, included both South and North (!) Koreas in the canonical territory of the MP.[13] Without a doubt, it was a demonstrative and preemptive action of the Moscow Patriarchate based on the conviction that, besides Ukraine, Constantinople also intends to take over MP's canonical territory in South-Eastern Asia (e.g., in China and Japan).[14] Especially interesting in this collision is the involvement on the side of Moscow of such a closed and communist country like North Korea.

In contrast to the People's Republic of China and Japan, the Statute of the ROC does not mention North Korea as part of its canonical territory. However, North Korea is listed in the digital maps of the ROC among the countries of the world that are comprised in the canonical jurisdiction of the Moscow Patriarchate; although the option "North Korea (DPRK)," available in the map settings, would not display any church objects in this country as of the date of this publication. This might lead to a provisional conclusion that the map option "North Korea" could be a technical "backlog" reserved for future updates.

Nevertheless, the Embassy of the Russian Federation in the DPRK on its official website maintains a webpage[15] dedicated to the newly-built Temple of the Life-Giving Trinity in Pyongyang.[16] According to the Embassy information, the Trinity Temple has been in the jurisdiction of the Moscow Patriarchate since 2006. Specifically, it is emphasized that Chairman of the DPRK Orthodox Committee (!) Ho Il Jin, sent a request to Patriarch Alexii II of the ROC in June 2006, asking him to receive the Life-Giving Trinity Temple into the canonical jurisdiction of the Russian Orthodox Church. It is no wonder that the parish in Pyongyang was readily accepted.[17] In 2018, the MP published unique high-resolution photographs of the first-ever visit of the DPRK Orthodox Committee to Moscow, where the Committee met with Patriarch Kirill.[18] The particulars of the highly interesting theopolitical relations of the North-Korean regime with Russian Orthodoxy, however, go beyond the scope of this article.

On 4th December 2018, the Russian Embassy in Pyongyang posted an unusual text on its official Facebook account.[19] Referring to the Trinity Temple, the Embassy notified: "We were so much surprised by the fact that, in the faraway Istanbul, they [the Ecumenical Patriarchate] seriously consider the Trinity Church in Pyongyang its own. At least, it follows so from the calendar published by the Korean Metropolis of the Patriarchate of Constantinople on the occasion of Patriarch Bartholomew's visit to Seoul."

Figure 1. *The Ecclesial Map of the Korean Peninsula*
Source: Russian Embassy in North Korea

Indeed, the picture of the calendar uploaded on Facebook contains an offline map of the Korean peninsula with Pyongyang marked as canonical territory of the Orthodox Metropolis of Korea of the Ecumenical Patriarchate. In Fig. 1, the image and the description of the Trinity Temple in Pyongyang are in the center of the calendar layout, immediately beneath the map of the Korean peninsula.

Above the Korean peninsula in the layout, there is an official web address of the Metropolis of Korea, *Orthodoxkorea.org*, in which both Pyongyang and the Trinity Temple are indicated as belonging to the canonical jurisdiction of Constantinople.[20] Moreover, and in contradiction to the information of the Russian Embassy in Pyongyang that the construction of the Temple was funded by North Korea and sponsored by Russia, the Metropolis argues to have provided assistance for the construction of the Temple in the North.

As the Russian Embassy further tells its Facebook readers, the Orthodox Committee of the DPRK has repeatedly explained to the representatives of Constantinople the status of the Temple of the Holy Trinity in Pyongyang, that is, it denied them the title to it. Besides, the Embassy draws a parallel with the ecclesial conflict in Ukraine, according to which, North Korea would not let Constantinople take over the MP's canonical territory in North Korea the way the EP has done in Ukraine. The posting by the Russian Embassy in Pyongyang, which uploaded the church-related map of the Korean peninsula (that was probably ob-

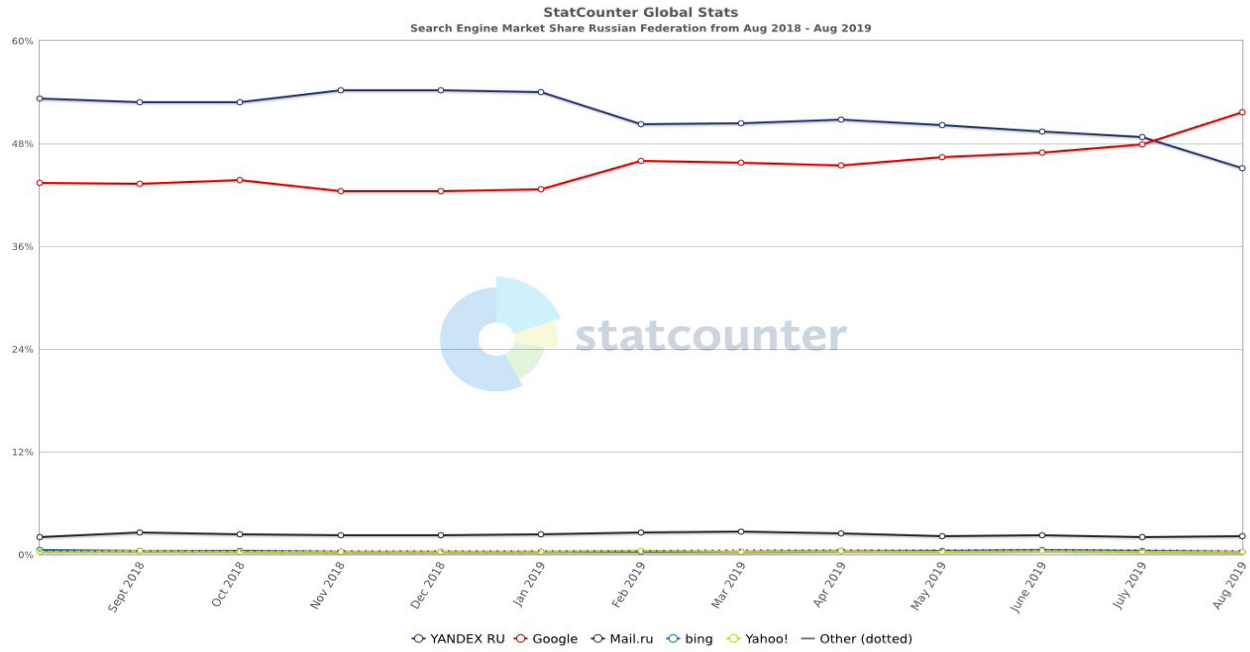


Figure 2. *Statistics on Yandex and Google in Russia*
Source: StatCounter

tained from the Orthodox Committee of the DPRK), thus brought the topic of canonical territory via Facebook to a larger audience; and it made quite a story in Russian digital media.[21]

Yandex Maps: The "Uploaded" Canonical Territory of the ROC

In June 2015, in implementation of Resolution 43 of the ROC Bishops' Council of 2013, *Prihod.ru* created and launched a digital map of ROC's canonical territory. The online map, *Prihod.ru/karta/karta-xramov*, currently exists as a beta-version and aims at "uploading" all MP's parishes and other church objects across the globe, based on the Russian search engine Yandex and the WordPress platform. Yandex, in general, and Yandex Maps, in particular, are powerful competitors to Google and Google Maps in the Russian Federation. For instance, according to the all-platforms statistics provided by StatCounter, Yandex outperformed Google by a rather thin margin between August 2018 and August 2019; although as per mobile search engine market share, Google was slightly ahead of Yandex.[22]

The maps of the ROC currently display over twenty thousand objects worldwide, subdivided into the ROC per se and the Russian Orthodox Church Abroad (ROCA), the latter being an autonomous unit within the MP. The mapping resource is maintained by the *Prihod.ru* network, whose information is used below. In order to be mapped, ROC parishes sign in, fill out, and upload the required information on *Prihod.ru*, after which their data is automatically integrated into the system. This means that the parish location displayed in Yandex Maps is the one entered during the initial registration. Whether it is accurate or not, depends on the concrete parish that signed in. There is no centralized catalog in this respect that would be controlled by the ROC; parishes can only receive instructions from above to sign in. If the information on the parish has changed, it should be edited by those who uploaded it, and the data will be updated automatically on all related websites within the system.

Icons like  mark various church objects. One object is symbolized by a single icon on the map, and a few objects in one area are portrayed by a circle with a digit inside, showing how many objects there are in the area, such as in the header picture.

By clicking on the map icons and by zooming in, Internet users can get an overview, in the form of a pop-up "business card," of this or that parish or temple and see its location in Yandex Maps. The "card" contains a telephone number and, often, a person in charge (in practice, it is usually a priest and his private cell-phone number), affiliation, and a link to the website of the mapped object, if available.

Users can surf the ROC maps by country or by church object. For instance, the option "Germany" displays one hundred eight ROC objects in this country as of the date of this publication. Furthermore, the map has an option called "Layers," containing four image versions: a standard map image, a satellite image, and a hybrid map; besides, there is a panorama view.

The Ukrainian Orthodox Church of the Moscow Patriarchate (UOC MP), being an autonomous church

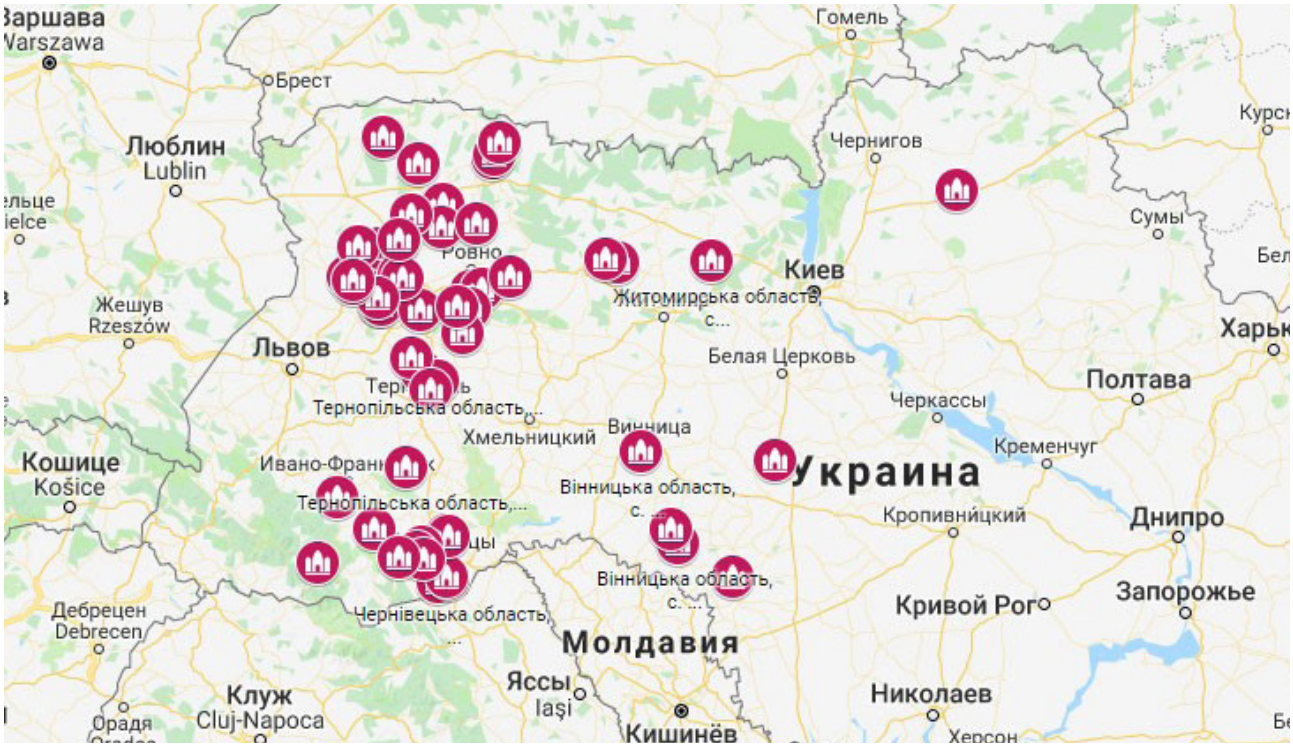


Figure 3. *Digital Map of Ecclesial Conflicts in Ukraine*
Source: Law.church.ua

within the MP, followed the digital trend of the Patriarchate and launched two similar digital maps on a local level. One of them, *Church.ua/karta*, is called Web-Atlas of the UOC MP. It is noteworthy that this web-atlas displays Ukraine *with* Crimea, as one integral canonical territory of Kiev; although the Russian Federation considers Crimea part of its state territory after 2014, the only canonical church present in Crimea is, in fact, the UOC MP and not the ROC per se.

Another digital initiative of the UOC MP is the scrupulous online mapping of church conflict areas in Ukraine in light of the unfolding conflict between Moscow and Constantinople. Its Juridical Department, *Law.church.ua*, created a map based on Google Maps.[23] The UOC MP uses various media reports, including witnesses on the ground, in order to swiftly map and present to a larger audience the cases of the church standoff and takeovers by the competing ecclesial organizations. As can be seen in Fig. 3, most takeovers are mapped in the (traditionally anti-Russian) West of Ukraine.

By clicking on the icons, Internet users get access to the information on the church conflict in that particular area with the indication of the source(s) and a description of the subject matter on the left-hand side of the screen. For instance, Internet users can post certain information on Facebook of which they have become aware, and the relevant link to it is provided in the description box. This initiative was designed as a protection policy of the UOC MP that "de-privatizes" the local conflicts in question and draws public attention to the church situation in the country in the *de facto* absence of institutional protection from the Ukrainian government. Unlike the ROC maps, the UOC MP project instrumentalizes the flip side of *Kartenpolitik*.

Conclusion

The intersection between the concept of canonical territory and online mapping in the activities of the Moscow Patriarchate creates a digital expression for its canon law. By "uploading" the canonical territory as GIS maps, the ROC engages in *Kartenpolitik*, the mapping project being not only *Orientierungshilfe* in the digital era but also its theopolitical and geotheological leverage. Besides, the ROC gives up its privacy (cf. *Religion ist Privatsache*) in favor of the "effective presence in the media"[24] and seeks additional ways to assure its territorial sovereignty, which is especially topical in the current jurisdictional conflict between Moscow and Constantinople. Despite being conservative in nature, the canon law herewith gains a new dimension in lockstep with digital modernity, whose implications for public and private life require critical reflection of experts on both religion and media.

Alexander Ponomariov

Postdoc am DFG-Graduiertenkolleg »Privatheit und Digitalisierung«.

Endnotes

1 For example: Suslov, Mikhail (ed.): *Digital Orthodoxy in the Post-Soviet World: The Russian Orthodox Church and Web 2.0.* Stuttgart: ibidem 2016.
2 Ponomariov, Alexander: The Body of Christ Online: The Russian Orthodox Church and (Non-) Liturgical Interactivity on the Internet. In: *Suslov 2016*, pp. 111–139.
3 For example: Hennermann, Karl: *Kartographie und GIS.* Darmstadt: WBG 2006, pp. 25–30.
4 Schneider, Ute: *Die Macht der Karten: Eine Geschichte der Kartographie vom Mittelalter bis heute.* Darmstadt: Primus Verlag 2006, p. 16.
5 For example: Happel, Jörn/Von Werdt, Christophe (eds.): *Osteuropa kartiert – Mapping Eastern Europe*. Münster: LIT 2010.
6 Schneider: *Die Macht der Karten*, p. 19.
7 Hilarion, Metropolitan: The Concept of "Canonical Territory" in Orthodox Tradition. A speech delivered at the international symposium "The Territorial and Personal Principles in Church Organization" at the Catholic University of Budapest, 7 February 2005. In: *Metropolitan Hilarion* published 25 February 2010, Online: http://old.hilarion.ru/2010/02/25/1048 (accessed 9 September 2019).
8 The Statute of the Russian Orthodox Church. The Russian Orthodox Church*: Department for External Church Relations.* Online: https://mospat.ru/en/documents/ustav/i/ (accessed 9 September 2019).
9 For example: Maximos, Metropolitan: *The Oecumenical Patriarchate in the Orthodox Church: A Study in the History and Canons of the Church*, translated from the Greek by Gamon McLellan. Thessaloniki: Patriarchal Institute for Patristic Studies 1976.
10 See the reiterated arguments of Constantinople: Sotiropoulos, Evangelos (ed.): *The Ecumenical Patriarchate and Ukraine Autocephaly: Historical, Canonical, and Pastoral Perspectives.* Order of Saint Andrew the Apostle: Archons of the Ecumenical Patriarchate in America 2019.
11 Bremer, Thomas/Senyk, Sophie: The Current Ecclesial Situation in Ukraine: Critical Remarks. In: *The St. Vladimir's Theological Quarterly*. Vol. 63, no. 1, 2019, pp. 27–58, here p. 27.
12 See: Ponomariov, Alexander: Theopolitics on the Grand Chessboard: Ukraine between the Church Canons and the Canons of War. *CEES Working Paper.* No. 2, 2019. University of Zurich: Center for Eastern European Studies, p. 10.
13 Internal Provision on the Patriarchal Exarchate of South East Asia. *Official Website of the Moscow Patriarchate* [in Russian], 26 February 2019; http://www.patriarchia.ru/db/text/5379645.html (accessed 9 September 2019).
14 Quan, Yuan: Interview with Dmitri Petrovsky: The U.S. is behind the Russian-Ukrainian Church Schism. In: *The Observer* [in Chinese] 17 December 2018. Online: https://www.guancha.cn/DmitriPetrovsky/2018_12_17_483490_s.shtml (accessed 9 September 2019).
15 The Orthodox Temple of the Life-Giving Trinity in Pyongyang. *Embassy of Russia to the DPRK* [in Russian]. Online: http://www.rusembdprk.ru/ru/rossiya-i-kndr/pravoslavnyj-khram-v-pkhenyane (accessed 9 September 2019).
16 Spiegel Online: *Kim Jong-Il and Religion: North Korea Builds an Orthodox Church* 11 August 2006. Online: https://www.spiegel.de/international/kim-jong-il-and-religion-north-korea-builds-an-orthodox-church-a-431310.html (accessed 9 September 2019).
17 Orthodox Church of the Life-Giving Trinity in Pyongyang. *Embassy of Russia to the DPRK.* Online: http://www.rusembdprk.ru/en/russia-and-dprk/orthodox-church-in-pyongyang (accessed 9 September 2019).
18 Meeting between Patriarch Kirill and Chairman of the DPRK Orthodox Committee. *Official Website of the Moscow Patriarchate, Press Service of the Patriarch of Moscow and All Rus'* [in Russian] 27 August 2018. Online: https://foto.patriarchia.ru/news/vstrecha-svyateyshego-patriarkha-kirilla-s-predsedatelem-pravoslavnogo-komiteta-kndr/ (accessed 9 September 2019).
19 Inappropriate Ambitions. Russian Embassy in the DPRK [in Russian]. In: *Facebook* published 4 December 2018, Online: https://www.facebook.com/RusEmbDPRK/photos/a.287010804806049/932993946874395/?type=3&__tn__=-R (accessed 9 September 2019).
20 Ambrose, Bishop/Zographos, Aristotle (Cho Song Am)/Metropolitan of Korea: Orthodox Witness in the Korean Peninsula: A Historical Approach. In: *Orthodox Metropolis of Korea*. Online: http://www.orthodoxkorea.org/history/ (accessed 9 September 2019).
21 For example: Lenta.ru: *Constantinople Wants to Take Away a ROC Temple in North Korea* [in Russian] 5 December 2018. Online: https://lenta.ru/news/2018/12/05/varfolomei/?fbclid=IwAR366Dih2JE_W5J3lRmzX4cajcdDR_k9nEPkJ0p9yfpIe0QnVX-U9Egs_4mk (accessed 9 September 2019).
22 StatCounter.com: *Search Engine Market Share Russian Federation: Aug 2018 – Aug 2019.* Online: https://gs.statcounter.com/search-engine-market-share/all/russian-federation (accessed 9 September 2019).
23 The UOC Information Center [in Ukrainian]: *The UOC Created a Map of Seized Parishes. 62 Parishes have been Seized.* In: Facebook published 26 March 2019. Online: https://www.facebook.com/788693681258269/posts/1973445299449762/ (accessed 9 September 2019).
24 Objectives of the Churchwide Information Policy [2013]. In: *Collection of Documents of the Russian Orthodox Church, vol. 2, part 2: Activities of the Russian Orthodox Church* [in Russian]. Moscow: The Moscow Patriarchy Press of the Russian Orthodox Church, 2014, pp. 629–630.

PUBLIKATIONEN AUS DEM KOLLEG

Aufsätze

Aldenhoff, Christian: Legitimation von Datenverarbeitung via AGB? Wider eine Verlagerung von datenschutzrechtlichen Abwägungen in das Vertragsrecht. In: Aldenhoff, Christian/Edeler, Lukas/Hennig, Martin/Kelsch, Jakob/Raabe, Lea/Sobala, Felix (Hg.): *Digitalität und Privatheit. Kulturelle, politisch-rechtliche und soziale Perspektiven.* Bielefeld: transcript Verlag 2019.

Gasiola, Gustavo Gil/Lopes, Juliano Marçal Lopes/Brandão Junior, Augusto Ferreira/Dias, Eduardo Mario: Smart Cities through Smart Regulation. In: *IEEE Technology and Society Magazine*. Jahrgang 38, Heft 1, S. 25-28. März 2019. doi: 10.1109/MTS.2019.2894457

Hauptmann, Kilian/Hennig, Martin: Alexa, optimier mich! KI-Fiktionen digitaler Assistenzsysteme in der Werbung. In: *Zeitschrift für Medienwissenschaft.* Jahrgang 11, Heft 21/2, 2019, Künstliche Intelligenzen, 86–94. doi: http://dx.doi.org/10.25969/mediarep/12636.

Hennig, Martin: Überwachung in der Kultur – Kultur der Überwachung. In: Liane Schüller/Werner Jung (Hg.): *Literatur und Überwachung*. Bielefeld: AISTHESIS 2019, S. 99-122

Hennig, Martin/Kelsch, Jakob/Sobala, Felix: ›Smarte Diktatur‹ oder ›egalitäre Netzgemeinschaft‹? Diskurse der Digitalisierung. In: Aldenhoff, Christian/Edeler, Lukas/Hennig, Martin/Kelsch, Jakob/Raabe, Lea/Sobala, Felix (Hg.): *Digitalität und Privatheit. Kulturelle, politisch-rechtliche und soziale Perspektiven.* Bielefeld: transcript Verlag 2019.

Heurich, Benjamin: Unsocial Bots – Eine Gefahr für die Autonomie des Gesellschaftssystems. In: Aldenhoff, Christian/Edeler, Lukas/Hennig, Martin/Kelsch, Jakob/Raabe, Lea/Sobala, Felix (Hg.): *Digitalität und Privatheit. Kulturelle, politisch-rechtliche und soziale Perspektiven.* Bielefeld: transcript Verlag 2019.

Jakobi, Hermann: Bavarian law on police as a new concept of legal security of Germany. In: Siberian Federal University (Hg.): *Law in a Digital Society: Transformation or modernization? Sammelband des V. Internationalen Rechtsvergleichungskongresses.* Krasnojarsk: Sibirische Bundesuniversität 2019. S. 158-165.

Kelsch, Jakob: Transparente Individuen im intransparenten System. Das Spannungsfeld von Privatheit und Digitalisierung in Marc-Uwe Klings Roman QualityLand. In: Aldenhoff, Christian/Edeler, Lukas/Hennig, Martin/Kelsch, Jakob/Raabe, Lea/Sobala, Felix (Hg.): *Digitalität und Privatheit. Kulturelle, politisch-rechtliche und soziale Perspektiven.* Bielefeld: transcript Verlag 2019.

Raabe, Lea: Die Kommentarspalten des Online-Magazins COMPACT als privatisierte Echokammer. In: Aldenhoff, Christian/Edeler, Lukas/Hennig, Martin/Kelsch, Jakob/Raabe, Lea/Sobala, Felix (Hg.): *Digitalität und Privatheit. Kulturelle, politisch-rechtliche und soziale Perspektiven.* Bielefeld: transcript Verlag 2019.

Riehm, Thomas/Meier, Stanislaus: Künstliche Intelligenz im Zivilrecht, in: DGRI-Jahrbuch 2018, Bd.028, 2019, S. 1-36.

Riehm, Thomas/Heiß ,Thomas A.: Aktuelle examensrelevante Rechtsprechung mit integriertem Falltraining, in: ZDRW Zeitschrift für Didaktik der Rechtswissenschaft, Jahrgang 6, Heft 3, S. 267 – 278.

Watzinger, Lea: Kritische Sichtbarkeit – Transparenz als opakes Konzept zwischen Selbst und Gesellschaft. In: *Allgemeine Zeitschrift für Philosophie: Primat des Praktischen. Zur Aktualität der griechischen Sophistik.* Heft 44.2, 2019, S. 225–228.

Monografien

Kelsch, Jakob: *Father Knows Worst! Familiendarstellung in der populärkulturellen US-amerikanischen Zeichentrick-sitcom*. Stuttgart: ibidem 2019.

Sammelbände

Aldenhoff, Christian/Edeler, Lukas/Hennig, Martin/Kelsch, Jakob/Raabe, Lea/Sobala, Felix (Hg.): *Digitalität und Privatheit. Kulturelle, politisch-rechtliche und soziale Perspektiven.* Bielefeld: transcript Verlag 2019.

Klepikova, Tatiana/Raabe, Lukas (Hg.): *Outside the »Comfort Zone«. Performances and Discourses of Privacy in Late Socialist Europe.* Oldenbourg: De Gruyter 2020.

Hennig, Martin/Schellong, Marcel (Hg.): *Überwachung und Kontrolle im Computerspiel.* Sonderausgabe »Paidia. Zeitschrift für Computerspielforschung« (in Vorbereitung).

ANKÜNDIGUNG

ERSCHEINT FRÜHJAHR 2020

NARRATIVE DER ÜBERWACHUNG

Kilian Hauptmann, Martin Hennig, Hans Krah (Hg.)
Peter Lang Verlag, Frankfurt am Main

Unter anderem durch kanonisierte Überwachungserzählungen der Literatur, wie etwa Aldous Huxleys *Schöne neue Welt* (1932) oder George Orwells *1984* (1948), gibt es eine Vielzahl von Motiven und Erzählungen der Überwachung, die in das Alltagswissen übergegangen sind und die kulturellen Verhandlungen und Vorstellungen von Sicherheit und Freiheit prägen. Wie dieser Band zeigt, finden sich aber auch einer Vielzahl von anderen Medien und Diskursen solche Narrative der Überwachung, wie etwa im Computerspiel, im Film, der Werbung oder in der Medien- und Aktionskunst.

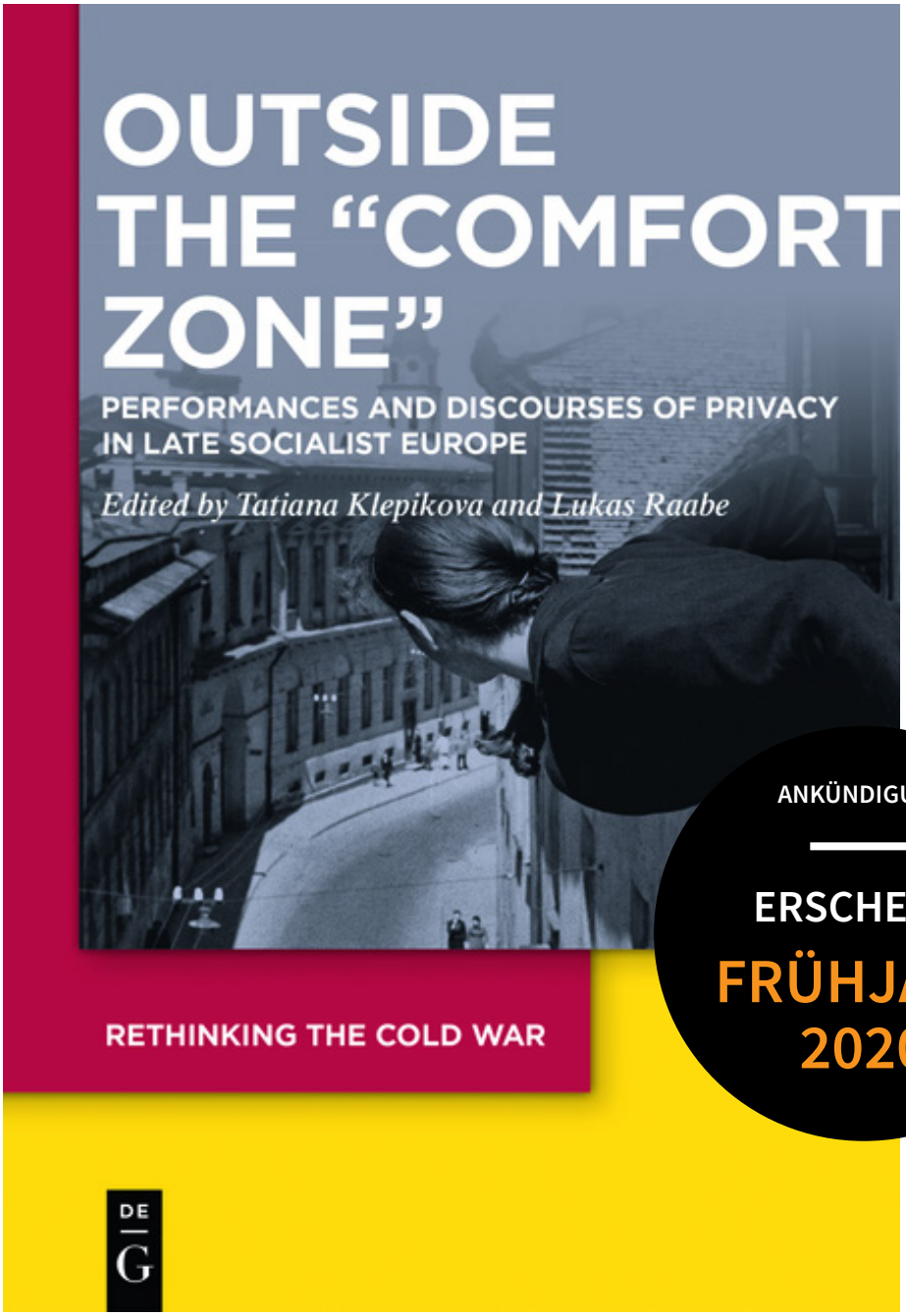
Der Band widmet sich diesen Modellierungen von Überwachung und geht Konstanten und Entwicklungen von Topoi, Motiven, Strategien und Diskursen anhand von verschiedenen Beispielen nach. Die kultur-, medien-, literatur-, und geschichtswissenschaftlichen Perspektiven der BeiträgerInnen nehmen dabei immer wieder das Verhältnis der Überwachungsnarrative zu Sicherheits-, Freiheits-, Privatheits- und Digitalisierungsdiskursen in den Blick.

Mit Beiträgen von:
Hans Krah, Martin Hennig, Dietmar Kammerer, Miriam Frank, Marcel Schellong, Sabrina Huber, Maren Conrad, Alix Michell, Thomas Christian Bächle und Lukas Raabe.

PUBLIKATIONEN AUS DEM KOLLEG

Datenschutz bleibt ein umkämpftes Thema im Kontext der voranschreitenden Digitalisierung. Die Beiträge des Bandes gehen der Frage nach, welche Formen Privatheit in einer digitalen Gesellschaft annehmen kann und welche Chancen und Risiken dabei entstehen. Dabei ergeben sich medienkulturelle Fragestellungen nach den Normierungsmustern hinter digitalen Anwendungen sowie die Notwendigkeit, digitale Nutzungsszenarien zu analysieren, einzuordnen und zu bewerten.

Link: https://www.transcript-verlag.de/media/pdf/51/c0/f9/oa9783839446614.pdf



ANKÜNDIGUNG

ERSCHEINT

FRÜHJAHR 2020

Traditionally, privacy studies have focused on the liberal democratic societies of the global West, whereas non-democratic contexts have played a marginal role in the discussion of the private and public spheres, not in the least because of the political stances of the Cold War era. This volume offers explorations of highly diversified performances and discourses of privacy by various actors which were embedded into the culturally, economically, and politically specific constructions of late socialism in individual states of the Warsaw Pact. Together, these articles document a palette of paradigms of the construction and transformation of the private spheres that overcame the national borders of individual states and left an imprint across the Eastern Bloc, thereby contributing to rethinking Cold War rhetoric in regard to these states. Link: https://www.degruyter.com/view/product/505437

VERANSTALTUNGSHINWEISE

17. Januar 2020

»COURTS AS LAW-MAKERS FOR THE INTERNET?«

Öffentlicher Gastvortrag mit Róberto Spanó (EuGH)

Hans-Bredow-Institut
Berlin

30. März - 2. April | Spring School »Own Data. Systems Medicine between Sovereignty and Solidarity«

Der Lehrstuhl für Systematische Theologie II (Ethik) der Friedrich-Alexander-Universität Erlangen-Nürnberg veranstaltet vom 30. März bis zum 02. April 2020 eine Spring School zum Thema »Own Data«. Das Ziel dieser Konferenz ist es, mit (Nachwuchs-)WissenschaftlerInnen über die rechtliche Handhabung personenbezogener, medizinisch relevanter Daten im klinischen und Forschungskontext zu diskutieren und die Ergebnisse in einen Sammelband zu publizieren.

Nürnberg, DE | frei

22.-24. Januar | CPDP2020 »Data Protection and Artificial Intelligence«

Die universitätsübergreifende Plattform CPDP lädt zum jährlichen Kongress in Brüssel ein. Die Non-Profit-Organisation bestehend aus 20 übergreifenden akademischen Zentren ist durch seine interdisziplinäre Ausrichtung wegweisend in den Themen Datenschutz und Privatheit. An diesen Tagen dreht sich alles um Datenschutz und künstliche Intelligenz.

Brüssel, BE | ab 100 €

13. März 2020

4. DIGITAL-MARKETING-KONFERENZ

Vorträge zu den Themen Automatisierung, KI, und Daten

Konferenz der Uni
Passau

13.-14. März 2020

SECURE SOCIETIES

Horizon 2020 Info Day and Brokerage Event

Brüssel, DE

2.-3. April | Frühjahrstagung »Künstliche Intelligenz und Weltverstehen«

Das Zentrum für Wissenschaftsforschung der Leopoldina lädt in Kooperation mit dem Interdisciplinary Network for Studies Investigating Science and Technology (INSIST) zu interdisziplinären Vorträgen ein. Es wird die KI als zentrale Schlüsseltechnologie der Gegenwart, mit der tiefgreifende gesellschaftliche und technische Veränderungen verbunden sind, betrachtet. Neben klassischen Vortrags- und Panelformaten soll dabei auch künstlerischen Einreichungen oder formal freieren Beiträgen (wie etwa Diskussionsrunden) Raum geboten werden. Eine Anmeldung ist nicht erforderlich.

Halle, DE | frei

DAS KOLLEG STELLT SICH VOR

Dr. Alexander Ponomariov

1. Am Kolleg seit? Juli 2019 als Postdoc.

2. Studiengang und Abschluss?

Russian and East Central European Studies, M.A., Passau.

Promotion (kanonisches Recht und Moderne im postsowjetischen Russland), Passau. Doktorvater: Prof. Dr. Dirk Uffelmann.

Ich hab dazu Orthodoxe Theologie in Moskau studiert. Ich habe z. B. das Vaterunser ins Hebräische des ersten Jahrhunderts n. Ch. rekonstruiert, siehe meine Fachpublikation »The Lord's Prayer in a Wider Setting: A New Hebrew Reconstruction«, *Journal of Northwest Semitic Languages*, 41-1/2015.

Davor habe ich Englisch und Deutsch als Fremdsprachen in der Ukraine studiert (Diplom).

3. Dissertationsthema

The Visible Religion: The Russian Orthodox Church and her Relations with State and Society in Post-Soviet Canon Law (1992–2015), Frankfurt am Main & New York: Peter Lang, 2017.

Meine Dissertationsschrift ist von Universitäten und Bibliotheken in unterschiedlichen Ländern von Deutschland bis Australien und Neuseeland bestellt worden, z. B. Uni Tübingen und LMU-München; Library of Congress und zwei Ivy League Unis: Yale University und University of Pennsylvania Law School (die sogenannte Penn Law); Università degli Studi di Padova; University of Queensland and Sidney University; Université du Québec; University of East Anglia.

4. Warum das GRK?

Eins meiner Forschungsinteressen ist die sogenannte »digitale Religion« und das GRK ist daher eine sehr gute Möglichkeit für diese Recherche. Darüber hinaus kann ich meine Betreuungserfahrungen und Kenntnisse auf Postdoc-Ebene anwenden.

5. Hätte ich nicht studiert, wäre ich gerne?

Das Leben wird leider bzw. glücklicherweise nicht in Konjunktiv II gelebt.

6. Ein Buch für die einsame Insel?

Neulich habe ich Erich Maria Remarque gelesen. Der war so populär in der Sowjetunion, dass jeder den Ausdruck *Im Westen nichts Neues* kennt. Seine Bücher sind »einsam« genug für die einsame Insel.

7. Ich gehe gerne…?

Zum Sport mehrmals pro Woche.

8. Ich esse gerne…?

Ich esse gerne, ja, das stimmt ☺.

9. Ich schaue gerne…?

Die »guten alten« Filme aus den 1990er Jahren, wie *Air America* mit Mel Gibson und Robert Downey jr.

Alexander Ponomariov

Postdoc am DFG-Graduiertenkolleg »Privatheit und Digitalisierung«.

TAGUNG DES KOLLEGS

Vier Jahreszeiten der Privatheitsforschung

Privatheit im Geflecht von Medien, Recht und Gesellschaft

Plenumsdiskussion der Tagungsgäste beim Panel »Privatheit und Transparenz als Normen«
Foto: Franziska Schönhöfer

von Marcel Schlegel

Es wurde konstruktiv diskutiert, die disziplinäre Brille getauscht – und ein bisschen wehten auch vier Jahreszeiten auf der Tagung »Verantwortung in digitalen Kulturen – Privatheit im Geflecht von Medien, Recht und Gesellschaft«, die vom 9. bis 11. Mai unter Leitung von Prof. Dr. Kai von Lewinski und Dr. Martin Hennig vom DFG-Graduiertenkolleg »Privatheit und Digitalisierung« in Passau stattfand.

TAGUNG DES KOLLEGS

Anfang Mai 2019 lud das DFG-Graduiertenkolleg »Privatheit und Digitalisierung« zu der interdisziplinären Tagung »Verantwortung in digitalen Kulturen – Privatheit im Geflecht von Medien, Recht und Gesellschaft« unter Federführung von Kollegsprecher Prof. Dr. Kai von Lewinski, Inhaber des Lehrstuhls für Öffentliches Recht, Medien- und Informationsrecht, und Dr. Martin Hennig, Post-Doc am Kolleg, ein.

Große Digitalkonzerne wie Facebook, Google oder Amazon, welche hinter den Sozialen Medien und virtuellen Plattformen stecken, durchdringen die Lebenswelten der meisten Bürgerinnen und Bürger mittlerweile schier umfänglich. In einem normativen Verständnis stellen Social Media dabei demokratiefördernde Diskursmedien dar, weil sie jenen egalitären öffentlichen Debattenraum bieten, in dem potenziell jede/r mit jeder/m diskutieren und auf diese Weise Meinungsvielfalt und Pluralismus florieren könnten – dies über nationale, kulturelle und jedwede hierarchisch konstituierte Grenzen hinweg. Dass dieses Ideal einer bunten virtuellen Austauschkultur bis dato weitgehend eine unerreichte Utopie geblieben ist, belegen nicht zuletzt aktuelle Fragen nach dem Schutz privater Informationen und Räume im Internet oder bisweilen populistisch motivierte Entwicklungen wie ›Hate Speech‹, ›Fake News‹ oder ›Social Bots‹, die diesen demokratischen Diskursraum gefährden oder bewusst vergiften – mit realen Gefahren für Autonomie und Demokratie.

Vor allem aber zeigt sich der Verlust des utopischen Leitbilds immer dann, wenn in gesellschaftlichen Debatten der Ruf nach staatlichen und rechtlichen Regulierung solcher ›Player‹ lauter wird, und wenn neben den angesprochenen Konzernen auch zivilgesellschaftliche, staatliche und politische Akteure in die Pflicht genommen und zum Handeln bewegt werden wie zuletzt etwa bei der EU-DSGVO. Dann bekommt die Frage nach der Verantwortung in der digitalen Sphäre einen konkreten Adressaten, den Staat.

Doch reicht der als Verantwortungsträger aus und inwieweit sollten Gesetzgeber selbst gesellschaftliche und wirtschaftliche Akteure verpflichten, die Gefahren digitaler Kulturen zu reflektieren und nicht zu missbrauchen? Um zu verhindern, dass die Utopie nicht zur Dystopie verkommt, braucht es offenbar ein allgemeines Verantwortungsbewusstsein maßgeblicher Akteure, sowie den aufklärerischen Blick jedes Einzelnen für all jene Aspekte der öffentlichen

Prof. Dr. Kai von Lewinski eröffnet die Tagung
Foto: Franziska Schönhöfer

Die KollegiatInnen des Kollegs »Privatheit und Digitalisierung« im Gespräch mit ReferentInnen
Foto: Franziska Schönhöfer

TAGUNG DES KOLLEGS

Digitalkultur, die statt Freiraum, Pluralismus und Debatte private Einschränkungen, individuelle Ausgrenzungen oder anti-demokratische Beschränkung bedeuten.

Vier Jahreszeiten der Privatheitsforschung

Mit einer Metapher eröffnete Prof. Dr. von Lewinski die Tagung: Als ›vier Jahreszeiten‹ umschrieb der Sprecher des DFG-Graduiertenkollegs die Veranstaltung. In seinem kurzen Vortrag zum Konferenzauftakt lieferte Professor von Lewinski, ebenso bildhaft gemeint, einen Klima- oder Wetterbericht zum inhaltlichen Status Quo der Privacy-Forschung im Allgemeinen und jenem des Graduiertenkollegs im Besonderen.

Wie auch Klima oder Wetter, so betreffen die in der Privatheitsforschung behandelten Themen weit mehr als nur einen kleinen fachspezifischen Dunstkreis an WissenschaftlerInnen. Im Gegenteil: Die Privacy-Forschung, die auch an der philosphischen und juristischen Fakultät der Universität Passau längst ihre Wurzeln geschlagen hat, behandelt Problemstellungen von zuweilen beträchtlicher Relevanz und Tragweite, denen sich mal Einzelne, mal Kollektive und nicht selten ganze Gesellschaften ausgesetzt sehen. Das zeigt sich zum Beispiel an aktuellen diskursiven Großwetterlagen, etwa an den Debatten um die EU-DSGVO oder um die gesellschaftliche Verantwortung großer Internetkonzerne wie Facebook oder Google.

Drei Tage, fünf Panels, 15 Vortragende

Dass sich derlei komplexe Fragen zur digitalen Umwälzung nur durch ein Zusammenspiel verschiedener Perspektiven beantworten lassen und damit ein interdisziplinärer Zugang besonders fruchtbare Erträge liefern kann, dürfte sich von selbst ver-

Wulf Loh in Diskussion mit den Gästen nach seinem Vortrag »Was sind soziale Pathologien der Privatheit?«
Foto: Franziska Schönhöfer

TAGUNG DES KOLLEGS

stehen. Entsprechend knüpften die Organisatoren der Passauer Tagung das Thema (digitale) Privatheit nicht nur an die Frage nach der Verantwortung, sondern verknüpften dieses Begriffspaar gleichsam mit verschiedenen Sichtweisen: der rechtlichen, politischen, ethischen, sozialen und auch ökonomischen.

Perspektiven, die sich auch in den fünf Panels und den so spannenden wie vielfältigen Vorträgen der insgesamt 15 Referentinnen und Referenten wiederfinden ließen. Diese widmeten sich in den von den Passauer Kollegiatinnen und Kollegiaten moderierten Zweier- oder Dreier-Sessions den Großthemen »Autonomie und Verantwortung in medialen Dispositiven«, »Staatliche und unternehmerische Verantwortung«, »Privatheit und Transparenz als ›Normen‹«, »Privatheit vs. Selbstverantwortung: gesellschaftliche Wertekonflikte« und »Anonymität, Freiheit und Verantwortung in digitalen Öffentlichkeiten«.

Frühling in der Privacy-Forschung

Und damit zurück zur Jahreszeiten-Metapher: Weil Fragestellungen zur »Privatheit und Digitalisierung« gesellschaftlich zunehmend bedeutsam geworden sind, erlebe auch die noch junge wissenschaftliche Disziplin der Privatheitsforschung in den letzten Jahren eine regelrechte Blütezeit. »Es ist Frühling in der Privatheitsforschung«, so Prof. von Lewinski. Dieses »Frühlingshafte« könne man selbstredend auch dem Passauer Graduiertenkolleg attestieren, an dem schließlich der Wissenschaftsnachwuchs mit der Erforschung des Stellenwerts des Privaten unter den Bedingungen von Digitalisierung und zunehmender informationeller Fremdbestimmung betraut ist.

Als Vortragende aus den Reihen der Kollegiatinnen und Kollegiaten bei der Tagung mit dabei: Lea Watzinger, Elizaveta Saponchik und Hermann

Foto: Franziska Schönhöfer

TAGUNG DES KOLLEGS

Jakobi, die den gut 50 Konferenzteilnehmenden Aspekte ihrer Promotionsvorhaben vorstellten (siehe nebenstehende Übersicht).

Sommerlicher Strauß an Themen

Kai von Lewinski jedenfalls sprach beim Blick ins Panel-Programm – seiner Metapher folgend – von einem »sommerlich bunten Strauß« an Privatheitsthemen, die von den angereisten WissenschaftlerInnen aus ganz Deutschland zunächst gepflanzt, durch konstruktive Gespräche auf der Konferenz gediehen seien und schließlich im geplanten Sammelband zur Tagung zur Blüte und Entfaltung kommen werden. »Im Herbst ist Erntezeit«, erklärte der Sprecher süffisant, um nicht zuletzt noch die Melancholie zu erwähnen, die der Herbstzeit bisweilen zu eigen ist.

Herbstlicher Abschied

Denn auch das DFG-Graduiertenkolleg »Privatheit und Digitalisierung« befinde sich gewissermaßen in seinem Herbst. Tatsächlich biegt das Kolleg in Passau, das von der Deutschen Forschungs-Gemeinschaft (DFG) seit 2012 gefördert wird, in seine Zielgerade ein; 2021 läuft die Förderung aus. Momentan forscht also der letzte Graduierten-Jahrgang am Kolleg. Doch an Abschied, das sprichwörtliche Jahresende und an den kalten Winter, der bevorstehe, wolle man noch gar nicht denken, so Professor von Lewinski. Er verwies stattdessen auf einige Panel-Vorträge, die vor allem gesellschaftspolitische Themen in den Fokus rückten, zum Beispiel Elizaveta Saponchik und Hermann Jakobis Vortrag zu »Ausweitung der Befugnisse russischer Sicherheitsorgane und Geheimdienste im Internet« – staatliche Privatheitsgefährdungen, bei denen ein »winterlich kalter Hauch« spürbar sei, so Kai von Lewinski. Metaphorisch gesprochen, versteht sich.

Marcel Schlegel

Wissenschaftlicher Mitarbeiter am DFG-Graduiertenkolleg »Privatheit und Digitalisierung«.

KollegiatInnen des Kollegs im Gespräch mit Tagungsgästen
Foto: Franziska Schönhöfer

Elizaveta Saponchik und Hermann Jakobi in Diskussion mit den Tagungsgästen
Foto: Franziska Schönhöfer

Dr. Tim Raupach im Vortrag »Big Data und die Produktion gesellschaftlicher Normalität«
Foto: Franziska Schönhöfer

TAGUNG DES KOLLEGS

Lea Watzinger im Interview über die Widersprüchlichkeit des Anonymitätsbegriffs.
Foto: Franziska Schönhöfer

Elizaveta Saponchik fragte nach der Verschlüsselung als Schutzgut des Grundrechts.
Foto: Franziska Schönhöfer

Hermann Jakobi über die Blockade ausländischer VPN-Dienste in Russland.
Foto: Franziska Schönhöfer

Die Beiträge der KollegiatInnen im Detail

Lea Watzinger beschäftigte sich in ihrem Vortrag »Namenlos, durch das Netz« mit zwei gegenläufigen Tendenzen digitaler Kommunikation: mit Anonymität und Transparenz. Anhand einer begrifflichen Gegenüberstellung zeigte die Philosophin die entscheidenden normativen Bedeutungsebenen auf und band diese an die Frage nach Verantwortung in digitalen Kulturen zurück. Bei beiden Phänomenen spielt die Frage nach der Verantwortung eine zentrale Rolle, zudem kommt ihnen eine hohe normative Strahlkraft zu: sie beschreiben nicht nur einen Zustand, sondern es stehen durchaus gegeneinander laufende Konzepte von Demokratie, Freiheit, und ‚dem guten Leben' dahinter.

Anonymität und Transparenz haben zudem mit der Digitalisierung an neuer Relevanz gewonnen: Einerseits scheint die digitale Kommunikation im Internet Anonymität zu ermöglichen, andererseits ermöglicht die Digitalisierung eine ungekannte Sichtbarmachung und Transparenz. Als philosophisch einordnenden Rahmen zog Lea Watzinger Vita activa von Hannah Arendt heran. Die Kollegiatin diskutierte dabei Arendts Problematisierung der Anonymität von Handelnden vor der Gegenfolie des liberalen Denkens.

In einem gemeinsamen Vortrag widmeten **Elizaveta Saponchik** und **Hermann Jakobi** sich einem aktuellen russischen Konflikt: jenem zwischen dem momentan in Russland gesperrten Messenger-Dienst *Telegram* und den staatlichen Sicherheitsorganen, insbesondere dem Geheimdienst FSB, dessen Überwachungsbefugnisse ausgeweitet wurden. Am Beispiel der Telegram-Sperre wurde die Wirkung neuer restriktiver internetbezogener Gesetze geschildert. Im sogenannten »Jarovaja-Gesetz« wurde ein Verantwortlichkeitssystem geschaffen, das bürgerliche Aktivitäten im Internet kontrolliert und dabei den Dienstleistungsanbietern eine wesentliche Rolle zuschreibt.

Das erklärte Ziel dieser Rechtsnormen sei die Vorbeugung terroristischer Gefahr. So werden Messenger-Dienste Teil dieses staatlichen Mechanismus, auch wenn sie in Russland nicht physisch präsent sind; sie werden durch die Anwendung ihrer Nutzer vor dem russischen Staat verantwortlich.

Anhand des Telegram-Falls kann man sehen, zu welchen Konfrontationen es kommen kann, wenn ein Messenger – eben wie *Telegram* – seine Verantwortlichkeit vor allem im Privatheitsschutz sieht.

Foto: Przemek Klos / stock.adobe.com

DFG Graduiertenkolleg Privatheit und Digitalisierung
UNIVERSITÄT PASSAU
DFG Deutsche Forschungsgemeinschaft
Projektnummer 164644301

Die Finanzierung dieses Magazins erfolgt aus Mitteln der Deutschen Forschungsgemeinschaft.

Das Magazin hat Ihnen gefallen?

Sie möchten das Magazin online abrufen oder sich zum regelmäßigen Empfang in den Verteiler eintragen? Besuchen Sie uns auf unserer Website: www.privatheit.uni-passau.de/magazin-des-graduiertenkollegs/

Für Hinweise, Anregungen, Lob und Kritik sind wir Ihnen sehr dankbar. Schreiben Sie einfach an privatheit@uni-passau.de

IMPRESSUM

Anschrift
Universität Passau
Innstraße 41
94032 Passau
Telefon: 0851/509-0
Telefax: 0851/509-1005
E-Mail: praesidentin@uni-passau.de
Internet: www.uni-passau.de
USt-Id-Nr.: DE 811193057

Redaktion
Dr. Jenny Bauer
Dr. Alexander Ponomariov
Kilian Hauptmann

Vertretung
Die Universität Passau wird von der Vorsitzenden des Leitungsgremiums, Präsidentin Prof. Dr. Carola Jungwirth, gesetzlich vertreten. Verantwortliche im Sinne des § 5 TMG (Telemediengesetz) ist die Präsidentin. Für namentlich oder mit einem gesonderten Impressum gekennzeichnete Beiträge liegt die Verantwortung bei den jeweiligen Autorinnen und Autoren.

Layout & Satz
Franziska Schönhöfer
Sadia Ouro-Gbele

Organisation
Gemäß Art. 4 Abs. 1 BayHSchG ist die Universität Passau als Hochschule des Freistaates Bayern eine Körperschaft des öffentlichen Rechts und zugleich staatliche Einrichtung. Aufsichtsbehörde ist das Bayerische Staatsministerium für Bildung und Kultus, Wissenschaft und Kunst in München (Anschrift: Salvatorstraße 2, 80333 München).

Bilquellen:
Colourbox.de
Stock.Adobe.de