Blockchain-Technologie im österreichischen E-Government:

eine Analyse des Rechtsrahmens ausgewählter Anwendungen mit einem verfassungsrechtlichen Fokus

Exposé über das geplante Dissertationsvorhaben

Verfasser:

Mag. Sascha Smets

angestrebter akademischer Titel

Doktor der Rechtswissenschaften (*Doctor iuiris*)

Wien, am 31.01.2019

Studienkennzahl lt. Studienblatt: A 783 101

Dissertationsgebiet: Öffentliches Recht / Verwaltungsrecht / Verfassungsrecht

Betreuer: Univ.-Prof. Mag. Dr. Christian M. Piska

I N H A L T S V E R Z E I C H N I S

1 Themengebiet des Dissertationsvorhabens

1.1 E-Government

Hintergründe

Vor etwas mehr als 25 Jahren machte sich eine neue Technologie auf, die Strukturen der öffentlichen Verwaltung nachhaltig zu verändern: das Internet. Dem World Wide Web entsprang die Vision der "Digitalen Stadt", die in Österreich erstmals 1995 unter der Leitung des damaligen "Internet"-Stadtrats der Stadt Wien, Hannes Swoboda, mit dem Projekt "Digitales Wien" unter der Internet-Adresse www.wien.at umgesetzt wurde, um Dienste der öffentlichen Verwaltung (wie etwa die digitale Stadtplansuche) digital abzubilden und den Wiener BürgerInnen anzubieten. Als weiterer großer Schritt wurden 1999 auch das Grund- und Firmenbuch über das Internet zugänglich und online abrufbar. Heute sind unzählige Verwaltungsangebote digital abrufbar und werden unter dem Sammelbegriff "E-Government" zusammengefasst.

In Österreich wir das gesamte eGovernment-Angebot vom Bundeskanzleramt unter der im Jahr 2005 geschaffenen Dachmarke "Plattform Digitales Österreich" gesamtheitlich koordiniert.[1] Die vom Bundeskanzleramt gewählte Definition für das E-Government impliziert bereits seine aktuelle und zukünftige Bedeutung: "*E-Government meint die Gesamtheit aller elektronischen Angebote der öffentlichen Verwaltung für die Menschen im Land und ist auch Synonym für einen modernen, transparenten und innovativen Staat, in dem Qualität, Vertrauen und Serviceorientierung zentrale Elemente sind.*"[2] Ziele des österreichischen E-Governments sind insbesondere die Effizienzsteigerung der öffentlichen Verwaltung, positive Auswirkungen auf den Wirtschaftsstandort Österreich und Steigerung des Sicherheitsniveaus der elektronischen Interaktion zwischen BürgerInnen, Unternehmen und Behörden.[3]

Rechtsrahmen

Den europäischen Rechtsrahmen für das österreichische E-Government bildet die Verordnung (EU) 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (eIDAS-VO). Die eIDAS-VO formuliert (i) Kriterien zu denen ein Mitgliedstaat verpflichtet ist, elektronische Identifizierungsmittel für natürliche und juristische Personen anzuerkennen und (ii) Mindestbedingungen für elektronische Signaturen und Dokumente sowie Zertifizierungsdienste. Es ist ein erklärtes Ziel der eIDAS-VO, ein angemessenes Sicherheitsniveau bei Vorgängen zur elektronischen Identitätsfeststellung zur Stärkung des

[1] Abrufbar unter https://www.digitales.oesterreich.gv.at.

[2] *Digitales Österreich*, Behörden im Netz: Das österreichische E-Government ABC, https://www.digitales.oesterreich.gv.at/documents/22124/30428/E-Government-ABC.pdf (31.01.2019).

[3] ErlRV 1145 BlgNR XXV. GP, 27.

Binnenmarkts zu schaffen.[4] Die eIDAS-VO greift allerdings inhaltlich nicht in bestehende elektronische Identitätsfeststellungssysteme der Mitgliedstaaten ein.[5]

Innerstaatlich ist das österreichische E-Government-Gesetz das regulatorische Kernstück. Es wurde mit BGBl. I Nr. 121/2017 grundlegend novelliert um (i) den Erfordernissen zur zwischenstaatlichen Anerkennung der elektronischen Identitätsfeststellung im Sinne der e-IDAS-VO zu entsprechen und (ii) das bislang bestehende System der Bürgerkarte[6] zu einem umfangreichen elektronischen Identitätsnachweis (E-ID) weiterzuentwickeln. Es folgten zwei kleinere Novellen[7] zur Herstellung der Konformität mit der Verordnung (EU) 2016/679 (DSGVO) und der Bundesministeriengesetz-Novelle 2017[8].

Die mit BGBl. I Nr. 121/2017 eingeführten Bestimmungen des E-Government-Gesetzes zur E-ID sind zum Zeitpunkt dieses Exposés noch nicht in Kraft getreten. Diese Bestimmungen sollen erst zum Zeitpunkt an dem die technischen und organisatorischen Voraussetzungen zum Echtbetrieb der E-ID gegeben sind in Kraft treten. Der entsprechende Zeitpunkt wird vom Bundesminister für Inneres im Bundesgesetzblatt kundgemacht werden. Für Zwecke dieses Exposés wird von einer entsprechenden Kundmachung und dem damit zusammenhängenden Inkrafttreten der Bestimmungen zur E-ID des E-Government-Gesetzes bis zur Fertigstellung des Dissertationsvorhabens ausgegangen.

Das E-Government fällt in die Zuständigkeit des Bundes in Gesetzgebung und Vollziehung.[9] Der einfachgesetzliche Rechtsrahmen des E-Governments wird insbesondere vom Signatur- und Vertrauensdienstegesetz (SVG), vom Allgemeinen Verwaltungsverfahrensgesetz (AVG) und vom Zustellgesetz (ZustG) komplettiert.

---

[4] Vgl Artikel 1 Verordnung (EU) 910/2014.

[5] ErwGr 13, 21 und 25 Verordnung (EU) 910/2014.

[6] Die Bürgerkartenfunktion kann auf unterschiedlichen Trägermedien (Chipkarte: "Bürgerkarte" oder Mobiltelefon: "Handysignatur") aktiviert werden. Sie beinhaltet eine qualifizierte, elektronische Signatur und kann damit zur Unterzeichnung von Dokumenten (in Gleichstellung zur handschriftlichen Unterschrift) verwendet werden. Vgl hierzu Digitales Österreich, Behörden im Netz: Das österreichische E-Government ABC, https://www.digitales.oesterreich.gv.at/documents/22124/30428/E-Government-ABC.pdf (30.01.2019).

[7] BGBl. I Nr. 32/2018 und BGBl. I Nr. 104/2018.

[8] BGBl. I Nr. 164/2017.

[9] 316/ME XXV. GP zu den zugrundeliegenden Kompetenzgegenständen (i.e. Datenschutz, Meldewesen, Passwesen und Bedarfsgesetzgebung für das Verwaltungsverfahren nach Art. 11 Abs. 2 B-VG).

Probleme des aktuellen E-Government-Angebots

Das österreichische E-Government hat mit zwei evidenten Problemen zu kämpfen[10]: mangelnde Nutzung durch die BürgerInnen sowie Gefahren und Risiken durch Cyberkriminalität[11] und Intransparenz. Die Verschachtelung dieser beiden Probleme zeigt folgende Statistik: lediglich ein Drittel der ÖsterreicherInnen haben die Bürgerkartenfunktion bislang freischalten lassen[12]. Besonders besorgniserregend ist die Quote bei den 18 bis 25-Jährigen: lediglich ein Viertel haben in dieser Altersgruppe die Bürgerkartenfunktion freischalten lassen.

Gründe für die geringe Nutzung, sind insbesondere die fehlenden Transparenz der E-Government-Angebote und Sicherheitsbedenken im Zusammenhang mit der zentralen Speicherung.[13] So hat auch die EU-Kommission in einer Mitteilung[14] die globale Cyberkriminalität als einer der größten "*Hemmnisse für den Erfolgszyklus der digitalen Welt*" identifiziert. Sichere und transparente E-Government-Angebote führen demnach zwangsläufig auch zu einer verstärkten Nutzung.

So wie das Internet vor 25 Jahren, steht auch heute eine Technologie in den Startlöchern, die die öffentliche Verwaltung in Österreich nachhaltig verändern und bereits bestehende E-Government-Angebote verbessern könnte: die Blockchain-Technologie. Die Blockchain-Technologie birgt insbesondere das Potential zentrale Datenregister gegen Eingriffe Dritter zu schützen, die Datenintegrität zu gewährleisten und so Vertrauen in elektronische Verwaltungsangebote in der Bevölkerung zu stärken.

---

[10] Vgl hierzu eGovernment Monitor 2018, https://www.egovernment-monitor.de/fileadmin/uploads/user_upload/studien/PDFs/191029_eGovMon2018_Final_WEB.pdf (30.01.2019).

[11] Wurden in Österreich im Jahr 2004 noch 753 Fälle von Cybercrime polizeilich angezeigt, waren es im Jahr 2017 bereits 16.804 (https://de.statista.com/statistik/daten/studie/294141/umfrage/cybercrime-in-oesterreich/ (24.01.2019)).

[12] In Deutschland sind es gerade einmal 22% (eGovernment Monitor 2018, https://www.egovernment-monitor.de/die-studie/2018.html).

[13] eGovernment Monitor 2018, https://www.egovernment-monitor.de/fileadmin/uploads/user_upload/studien/PDFs/191029_eGovMon2018_Final_WEB.pdf (30.01.2019); Vgl ErwGr 1 VO (EU) 910/2014.: "*Die wirtschaftliche und soziale Entwicklung setzt Vertrauen in das Online-Umfeld voraus. Mangelndes Vertrauen führt dazu, dass Verbraucher, Unternehmer und öffentliche Verwaltungen nur zögerlich elektronische Transaktionen durchführen oder neue Dienste einführen bzw nutzen, vor allem wenn sie die Befürchtung hegen, dass es an Rechtssicherheit mangelt.*"

[14] KOM/210/0245 endg.

1.2 Blockchain[15]

Technische Einleitung[16]

Eine Blockchain ist – vereinfacht ausgedrückt – eine unveränderliche, dezentrale Datenbank von verschiedenen, gleichberechtigten, Computern (so genannten "Nodes") ohne zentrale Instanz oder Server. Neue Datenbankeinträge werden zunächst an alle Nodes im Blockchain-Netzwerk verteilt und von den Nodes nach bestimmten, im Quellcode der Blockchain vorgegebenen Kriterien inhaltlich geprüft. In weiterer Folge werden die Datenbankeinträge (i) von Minern (nachfolgend beschrieben) in Datenblöcken zusammengefasst, (ii) in Standartwerte (so genannte "Hashwerte") kodiert und (iii) mit einem Zeitstempel versehen. Derselbe Datenbankeintrag kann dabei nur einmal im selben Block vorkommen.[17]

Die kodierten Datenblöcke sind gegenüber Manipulationsversuchen sicher, da eine Manipulation der ursprünglichen Information zu einem stark veränderten Hashwert führt. Jeder nachfolgende Datenblock ist durch den Hashwert mit dem vorherigen Block "verkettet" und trägt damit die gehashte Datenbankhistorie mit sich. Die Hashwerte der kodierten Datenblöcke können dann von sämtlichen Nodes überprüft werden. Miner sind Nodes, die Rechenleistung zur Verfügung stellen um die Datenbankeinträge in Blöcken zusammenzufassen und Hashwerte für diese Blöcke zu berechnen. Die Miner erhalten für die erfolgreiche Berechnung des Hashwerts für einen Datenblock eine Belohnung. Welcher Miner den Hashwert für einen Block nun tatsächlich als erster berechnet ist eine reine Wahrscheinlichkeitsrechnung – je mehr Rechenleistung ein Miner hat, desto eher wird er der erste Miner sein, der den korrekten Hashwert berechnet (so genanntes Proof-of-Work-Verfahren)[18]. Das erfordert ein enormes Maß an Rechenleistung. Es gibt allerdings bereits eine Vielzahl von

---

[15] Die nachfolgende Beschreibung der Blockchain-Technologie soll lediglich einen technischen Überblick über das Themengebiet für Zwecke dieses Exposés verschaffen und hat keineswegs den Anspruch eine vollständige technische Abhandlung dieser komplexen Technologie zu sein.

[16] *Müller*, Bitcoin, Blockchain und Smart Contracts, ZfIR 17-18/2017; *Kreuzer*, Was ist eine Blockchain?, CFOaktuell 2017, 109; *Blocher*, The next big thing: Blockchain – Bitcoin – Smart Contracts, AnwBl (dt) 8+9/2016; *Spancken*/*Hellenkamp*/*Brown*/*Thiel*, Kryptowährungen und Smart Contracts, https://www.hb.fh-muenster.de/opus4/frontdoor/deliver/index/docId/920/file/FuE_Kryptowaehrungen_und_Smart_Contracts_Abschlussbericht.pdf (30.01.2019); Fraunhofer, Blockchain und Smart Contracts, https://www.fraunhofer.de/content/dam/zv/de/forschung/artikel/2017/Fraunhofer-Positionspapier_Blockchain-und-Smart-Contracts_v151.pdf (30.01.2019); *Schrey*/*Thalhofer*, Rechtliches zur Blockchain, NJW 20/2017.

[17] Dadurch kann ein und derselbe Datenbankeintrag nur einmal vorgenommen werden.

[18] Das erste und derzeit auch noch beliebteste Konsensfindungsverfahren. Es kommt aktuell bei den zwei größten Blockchains zur Anwendung: Bitcoin und Ethereum. Ethereum stellt seine Konsensfindung allerdings schrittweise auf Proof-of-Stake um (siehe https://www.btc-echo.de/proof-of-stake-dank-casper-die-zukunft-vom-ethereum/ (30.01.2019)). Ob und wie Miner incentiviert werden und welcher Konsensfindungsmechanismus verwendet ist bei jeder Blockchain unterschiedlich. Bei maßgescheiderten Blockchain-Lösungen können diese Grundparameter (ebenso wie wer Zugriff hat und wer Datenbankeinträge hinzufügen darf) frei gewählt und angepasst werden.

energieschonenderen Alternativen, die bereits bei existierenden Blockchains im Einsatz sind.[19] Nachdem der Hashwert für einen Block durch einen Miner gefunden wurde, wird er an alle Nodes im Blockchain-Netzwerk kommuniziert. Daraufhin überprüfen die Nodes den Hashwert des Blocks und hängen ihn nach erfolgter Validierung an ihre lokale Blockchain an.

Zur aktiven Teilnahme an einem Blockchain-Netzwerk[20] als Node benötigt man lediglich ein kryptographisches Schlüsselpaar und eine Software, die den Teilnehmer mit dem Blockchain-Netzwerk verbindet. Beides wird in der Praxis durch so genannte Wallet-Programme ermöglicht.

Das Schlüsselpaar besteht aus den folgenden zwei Schlüsseln:

(i) der private Schlüssel mit dem neue Datenbankeinträge elektronisch signiert, verschlüsselt und an die Blockchain übermittelt werden können, wobei der private Schlüssel nur dem betroffenen Blockchain-Teilnehmer bekannt ist; und

(ii) der öffentliche Schlüssel, der, je nachdem ob es sich um eine private oder öffentliche Blockchain handelt (siehe unten), öffentlich bzw nur von den Blockchain-Teilnehmern einsehbar ist und mit dessen Hilfe mathematisch überprüft werden kann, dass der Datenbankeintrag tatsächlich vom dazugehörigen privaten Schlüssel signiert wurde. Die verschlüsselten Daten können nur mit dem privaten Schlüssel entschlüsselt werden. Vom öffentlichen Schlüssel kann nicht auf den privaten Schlüssel geschlossen werden.

Die aktuellste Fassung der Blockchain wird bei allen Nodes lokal abgespeichert. Dadurch vermeidet man per Design einen Single Point of Failure[21]. Die Nodes vergleichen ihre lokalen Blockchain-Versionen untereinander um die längste Blockchain festzustellen, die dann als allgemein gültig angesehen wird. Dadurch wird vermieden, dass zwei Versionen der selben Blockchain nebeneinander existieren können. Die bereits validierten Datenbankeinträge der kürzeren und damit ungültigen Blockchain-Versionen werden erneut validiert, in einem Block gesammelt und an die längste Blockchain angeschlossen, soweit sie darin nicht bereits enthalten sind.

Die Sicherheit und Integrität einer Blockchain steht demnach auf fünf Pfeilern:

(i) die digitale Signatur durch den privaten Schlüssel gewährleistet, dass ein Datenbankeintrag vom tatsächlich Berechtigten stammt,

(ii) die Kodierung der Datenbankeinträge in Hashwerte schützt vor nachträglicher Veränderung der Daten,

---

[19] Allen voran das Proof-of-Stake-Verfahren, durch das Rechenleistung und damit der Energieverbrauch auf ein Minimum reduziert werden soll.

[20] Z.B.: Datenbankeinträge erstellen, digitale Vermögensgüter empfangen und übertragen, etc.

[21] Vgl hierzu https://de.wikipedia.org/wiki/Single_Point_of_Failure: "*Unter einem Single Point of Failure versteht man einen Bestandteil eines technischen Systems, dessen Ausfall den Ausfall des gesamten Systems nach sich zieht.*".

(iii) das lokale Abspeichern der Blockchain-Versionen bei jedem Node und ein allgemeiner Konsens darüber, welche Blockchain-Version gültig ist, vermeidet einen Single Point of Failure und abweichende Blockchain-Versionen,

(iv) der Konsensfindungsprozess zur inhaltlichen Validierung der Datenbankeinträge, und

(v) die Vermeidung des Double Spending[22] durch die Zusammenfassung der Datenbankeinträge in Blöcke mit der Maßgabe, dass derselbe Datenbankeintrag nicht zweimal in einem Block vorkommen kann (dadurch schafft es ein Datenbankeintrag auch nur einmal in die Blockchain).

Blockchain-Arten[23]

Die Teilnahme (wie etwa die Erstellung von Datenbankeinträgen) an einer Blockchain kann beschränkt werden. So spricht man bei Blockchains, bei denen es keine Teilnahmebeschränkungen gibt, von "permissionless Blockchains" und bei Blockchains, bei denen lediglich ausgewählte Teilnehmer Datenbankeinträge erstellen dürfen, von "permissioned Blockchains". Weiters kann im Quellcode der Blockchain festgelegt werden, ob die Blockchain von jedermann ("öffentliche Blockchain") oder nur von einem bestimmten Personenkreis eingesehen werden kann ("private Blockchain").

Smart Contracts

Zur Erweiterung der Funktionalität der Blockchain-Technologie ermöglichen unzählige Blockchain-Plattformen (wie etwa Ethereum) die Programmierung und den Einsatz so genannter Smart Contracts. Ein Smart Contract ist ein Programmcode, der Wenn-Dann Funktionen festlegt, die automatisiert von der Blockchain ausgeführt, nach den oben beschriebenen Verfahren validiert und auf der Blockchain gespeichert werden (nach dem Schema: wenn Bedingung A erfüllt ist, wird Operation B automatisch ausgeführt).[24]

1.3 Einsatz der Blockchain-Technologie im E-Government

Aufgrund der technischen Vorteile der Blockchain-Technologie finden sich im internationalen Umfeld bereits eine Vielzahl von Pilotprojekten im öffentlichen Sektor. [25] Datenbanken und Prozesse, bei denen Vertrauen und Datenintegrität essentiell sind,

[22] Ein- und dieselbe Transaktion wird gleichzeitig validiert und zweimal in die Blockchain aufgenommen.

[23] *Raffling*/*Schock* (Hrsg), Digitale Wirtschaft und Industrie 4.0 (2018) 167ff.

[24] Vgl zur Einschätzung von Smart Contracts im österreichischen Zivilrecht: *Smets*/*Kapeller*, Smart Contracts: Vertragsabschluss und Haftung, ÖJZ 2018/39; und zur Einschätzung im deutschen Zivilrecht: *Kaulartz*/*Heckmann*, Smart Contracts – Anwendungen der Blockchain-Technologie, CR 9/2016.

[25] Das Bundeskanzleramt hat in einer Präsentation die wichtigsten internationalen Pilotprojekte zusammengefasst: https://www.digitales.oesterreich.gv.at/documents/22124/403400/20170622-Blockchain-Village_BKA-Praesentation.pdf/6087cc17-4461-4b1b-a527-5bfd53703888 (30.01.2019).

könnten – zumindest theoretisch – von der Blockchain-Technologie profitieren. Auch in Österreich gab es hierzu ein erstes Pilotprojekt, bei dem Open Government Data[26] der Stadt Wien in Hashwerte kodiert und diese Hashwerte in mehreren öffentlichen Blockchains[27] gespeichert wurden.[28] Dadurch erhält der Hashwert (und die damit kodierte Information) einen Zeitstempel durch den geprüft werden kann, ob die Daten zu diesem Zeitpunkt tatsächlich so existiert haben. Jede Änderung dieser Daten ist dann transparent auf der Blockchain nachvollziehbar. Durch die dezentrale Struktur jeder einzelnen Blockchain und der Verteilung der Daten auf vier verschiedene Blockchains wird ein Single Point of Failure auf mehreren Ebenen vermieden und die Datenintegrität gewährleistet. Derartige Projekte zeigen das Potential der Technologie bei zentralen Registern. Darauf aufbauend lassen sich durch den Einsatz von Smart Contracts komplexe, automatisierte Prozesse (wie etwa die Stimmabgabe bei einer Wahl oder die Zustellung behördlicher Dokumente) transparent und sicher umsetzen.

Zentrale Register

Die Basis für funktionierende E-Government-Dienste ist die sichere Identitätsfeststellung von StaatsbürgerInnen, Unternehmen und Verwaltungsbehörden in der elektronischen Kommunikation untereinander. Österreich setzt hierzu auf die E-ID, eine Weiterentwicklung der Bürgerkartenfunktion[29], die auf Basis der e-IDAS-VO und des E-Government-Gesetzes implementiert werden soll. Durch die E-ID soll eine unverwechselbare, eindeutige Identität des Betroffenen geschaffenen werden, indem dem Betroffenen eine Stammzahl zugewiesen wird. Die Stammzahl wird (i) bei natürlichen Personen, die im ZMR[30] eingetragen sind, aus der ZMR-Zahl, und (ii) bei juristischen Personen aus der Firmenbuchnummer, durch kryptographische Verfahren rechnerisch gebildet.[31] Bei nicht meldepflichtige Personen (zB AuslandsösterreicherInnen), die sich freiwillig im eigens dafür eingerichteten Ergänzungsregister angemeldet haben, wird die Stammzahl aus der bei Eintragung im Ergänzungsregister gebildeten Ordnungsnummer errechnet.[32] Die Errechnung der Stammzahl erfolgt

[26] Öffentlich zugängliche, kostenlose und jederzeit verfügbare Daten der Verwaltung wie etwa Radwege oder Routen öffentlicher Verkehrsmittel; zugänglich unter https://www.data.gv.at/.

[27] Hierzu wurden die Blockchains Ethereum, Bitcoin, Litecoin und Ethereum Classic genutzt.

[28] https://digitales.wien.gv.at/site/1-blockchain-pilot-ogd-aenderungsprotokoll-und-notarization/ (24.01.2019).

[29] Die Kernelemente der Bürgerkartenfunktion (i.e. qualifizierte, elektronische Signatur und Personenbindung durch Zuweisung einer Stammzahl) bleiben demnach erhalten. Die Bürgerkartenfunktion wird durch die E-Government-Gesetz-Novelle 2018 derart erweitert, dass sie in den anderen EU-Mitgliedstaaten Anerkennung im Sinne der e-IDAS-VO findet. Weiters soll mit der E-ID die Basis für eine sichere, elektronische Identitätsfeststellung im privaten Bereich (zB zwischen Unternehmer und Verbraucher) geschaffen werden; vgl hierzu 316/ME XXV. GP.

[30] Zentrales Melderegister iSd § 16 MeldeG.

[31] § 6 Abs 2 und Abs 3 E-Government-Gesetz.

[32] § 6 Abs 4 E-Government-Gesetz.

durch das Bundesministerium für Digitalisierung und Wirtschaftsstandort als zuständige Stammzahlenregisterbehörde.[33] Die Stammzahlenregisterbehörde prüft bei der Bildung einer Stammzahl nicht die Korrektheit oder die Integrität der Daten, die zur Stammzahlbildung verwendet werden.[34] Daraus folgt: die Integrität und Sicherheit der elektronischen Identität jeder natürlichen oder juristischen Person hängt damit von der Integrität und Sicherheit des Melde- und Ergänzungsregisters sowie des Firmenbuchs und der dort zentral gespeicherten Daten ab.

Die in der österreichischen Strategie für Cyber-Sicherheit enthaltene Cyber-Risikomatrix weist einzelnen Cyber-Risiken eine Eintrittswahrscheinlichkeit (von sehr gering bis sehr hoch) und einen Intensitätsgrad der Auswirkungen (von begrenzt bis katastrophal) zu.[35] Dem Bedrohungsszenario "Manipulation von Bürgerdaten" wurden katastrophale Auswirkungen bei gleichzeitiger geringer Eintrittswahrscheinlichkeit zugemessen. Der Diebstahl digitaler Identitäten wurde als sehr wahrscheinlich eingeschätzt und mit erheblichen Auswirkungen verbunden. Die Risikomatrix verdeutlicht, dass – neben der bereits erfolgten Sensibilisierung und strategischen Neuausrichtung der Cyber-Sicherheits-Strategie des Bundes – konkretes Handeln des Gesetzgebers und/oder der Verwaltung in Bezug auf eine konkrete, technologische Weiterentwicklung bestehender Systeme notwendig sein könnte. Die Chance und Notwendigkeit Blockchain-Technologie als Prävention gegen Cyberangriffe einzusetzen erkannte auch Estland nachdem das Land im Jahr 2007 Opfer wochenlanger Cyberangriffe gegen staatliche Organe, Ministerien und Banken wurde.[36] Seit 2008 forscht die estnische Regierung an Einsatzmöglichkeiten der Blockchain-Technologie.[37] Seit 2012 wird die Blockchain-Technologie in den estnischen Registern zur Gewährleistung der Cybersicherheit eingesetzt.[37]

Die technische Umsetzung einer Blockchain-basierten Backup-Lösung für das Firmenbuch und das ZMR könnte dem erfolgreichen Pilotprojekt der Stadt Wien zu Open Government Data ähneln.[38]

---

[33] § 7 E-Government-Gesetz.

[34] Vgl 316/ME XXV. GP.: "*Da für die Richtigkeit dieser Daten aber jener Auftraggeber des öffentlichen Bereichs aus dessen Register diese Merkmale bezogen wurden verantwortlich ist, kann die Stammzahlenregisterbehörde mit ihrem Siegel lediglich die unversehrte Einfügung dieser Merkmale in die Personenbindung bestätigen.*"

[35] https://www.bundeskanzleramt.gv.at/documents/131008/780563/%C3%96sterreichische+Strategie+f%C3%BCr+Cyber+Sicherheit/3b007321-5d48-4a6e-8862-3f88d6a94116 (28.01.2019).

[36] https://de.wikipedia.org/wiki/Internetangriffe_auf_Estland_2007 (25.01.2019).

[37] https://e-estonia.com/ (25.01.2019).

[38] Wobei im Dissertationsvorhaben darauf eingegangen wird, dass permissioned Blockchains eher für den Einsatz bei E-Government-Anwendungen geeignet sind als permissionless Blockchains, die beim Open Government Data Projekt zum Einsatz gekommen sind.

E-Zustellung und E-Voting

Laut einer aktuellen Experten-Befragung zum Thema E-Government und Blockchain ist der Einsatz der Blockchain-Technologie in der österreichischen Verwaltung in den folgenden Bereichen denkbar bzw sinnvoll: Zentrale Register, E-Zustelldienste und E-Voting.[39] Hauptargumente hierfür sind insbesondere die Erhöhung der Datenqualität für zentrale Register, die Möglichkeit der transparenten Nachverfolgung bei E-Zustelldiensten sowie Transparenz und Unveränderlichkeit für E-Votings.[39] Die Bereiche E-Voting und E-Zustellung in Kombination mit der Blockchain-Technologie werden daher ebenfalls im Zentrum zweier Forschungsfragen des Dissertationsvorhabens stehen (siehe Punkt 2.3 und 2.4).

Grundbuch

Einem weiteren, potentiellen Einsatzgebiet der Blockchain-Technologie werden hingegen wenige Chancen eingeräumt: dem Grundbuch. Ausschlaggebend dafür sind viele offene technische Fragen und die Inkompatibilität mit dem österreichischen Grundbuchsystem.[40] In der deutschen Literatur werden ähnliche Argumente herangezogen um einen potentiellen Einsatz der Blockchain-Technologie im deutschen Grundbuch-System zu verneinen.[41] Internationale Pilotprojekte, wie etwa in Schweden[42], Estland[43] oder Georgien[44], zeigen allerdings durchaus sinnvolle Einsatzmöglichkeiten der Blockchain-Technologie für die entsprechenden nationalen Grundbuchsysteme auf. Von einer wissenschaftlichen Behandlung eines möglichen Blockchain-basierten Grundbuchsystems im Rahmen des Dissertationsvorhabens wird, aufgrund der derzeit unüberwindbaren Hindernisse einer technischen Umsetzung der Blockchain-Technologie im bestehenden Grundbuchssystem Österreichs, abgesehen.

2 Forschungsfragen

Das oben beschriebene Themengebiet und der damit gezimmerte Forschungsrahmen sind die Basis für die folgenden Forschungsfragen, die im Dissertationsvorhaben wissenschaftlich behandelt und beantwortet werden sollen:

---

[39] *Ollrom*, Auswirkungen von Blockchains auf die E-Government-Services des Bundes: Evolution oder Revolution, < http://pub.fh-campuswien.ac.at/obvfcwhsacc/download/pdf/2063683?originalFilename=true> (29.01.2019).

[40] https://www.addendum.org/blockchain/verwaltungsreform/ (30.01.2019); *Ollrom*, Auswirkungen von Blockchains auf die E-Government-Services des Bundes: Evolution oder Revolution, http://pub.fh-campuswien.ac.at/obvfcwhsacc/download/pdf/2063683?originalFilename=true (29.01.2019).

[41] *Wilsch*, die Blockchain-Technologie aus der Sicht des deutschen Grundbuchrechts, DNotZ 2017, 761.

[42] https://www.btc-echo.de/schweden-nutzt-jetzt-offiziell-die-blockchain-fuer-grundbucheintragungen/ (30.01.2019).

[43] https://e-estonia.com/wp-content/uploads/faq-a4-v02-blockchain.pdf (30.01.2019).

[44] https://www.bitcoinblase.at/blockchain-grundbuch-georgien-und-schweden-vorn/ (30.01.2019).

2.1 Bietet das NISG[45] (vor dem Hintergrund der NIS-Richtlinie[46]) einen konkreten[47] gesetzlichen Rahmen für den Einsatz der Blockchain-Technologie[48] als dezentrale Backup-Lösung für die Firmenbuchdatenbank und das ZMR?

Vorfrage

Um zur eigentlichen Forschungsfrage durchzudringen, wird im Dissertationsvorhaben die folgende Vorfrage behandelt werden: Gibt es bereits einen ausreichenden gesetzlichen Rahmen im Lichte von Artikel 18 B-VG auf Basis dessen die zuständigen Bundesverwaltungsbehörden die Blockchain-Technologie als Backup-Lösung für die Firmenbuchdatenbank[49] und das ZMR einsetzen können. Mit vorausschauendem Blick auf das IKT-Konsolidierungsgesetz, das Meldegesetz und das Firmenbuchgesetz ist hier von einem negativen Ergebnis auszugehen. Ein möglicher einfachgesetzlicher Rahmen könnte allerdings aufgrund des NISG bestehen.

NIS-Richtlinie und NISG

Die NIS-Richtlinie bildet den europarechtlichen Rahmen für Cybersicherheit in Europa. In Österreich soll die Richtlinie mit dem NISG umgesetzt werden.[50] Die NIS-Richtlinie verpflichtet die Mitgliedstaaten eine nationale Strategie für die Sicherheit von Netz- und Informationssystemen festzulegen und der EU-Kommission mitzuteilen. Eine derartige nationale Strategie hat unter anderem eine Angabe der Forschungs- und Entwicklungspläne im Zusammenhang mit der nationalen Strategie für die Sicherheit von Netz- und Informationssystemen zu beinhalten. Der Ministerialentwurf des österreichischen NISG weist dem Bundeskanzler die strategischen und dem Bundesminister für Inneres die operativen Aufgaben in Bezug auf die nationale Cybersicherheits-Strategie zu. Weiters werden drei Kategorien von Rechtssubjekten festgelegt, die vom NISG erfasst sein sollen: (i) Betreiber wesentlicher Dienste, (ii) Anbieter digitaler Dienste und (iii) Einrichtungen des Bundes. Jeder der Genannten wird unter dem NISG verpflichtet, im Hinblick auf die von ihnen betriebenen Dienste, die "dem Stand der Technik entsprechende Sicherheitsvorkehrungen

[45] Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz); liegt aktuell nur als Ministerialentwurf vor: 78/ME XXVI. GP. Für Zwecke dieses Exposés wird davon ausgegangen, dass das NISG bis zur Fertigstellung des Dissertationsvorhabens in Kraft getreten sein wird.

[46] Richtlinie (EU) 2016/1148.

[47] iSd § 18 B-VG.

[48] Mit "Einsatz der Blockchain-Technologie in zentralen Registern" soll lediglich der Einsatz als dezentrale Datenbank im Hintergrund eines bestehenden, zentralen Registers gemeint sein, auf der lediglich die Hashwerte der im zentralen Register gespeicherten Daten dezentral abgelegt und dadurch unveränderlich gespeichert werden sollen. Im Dissertationsvorhaben soll daher nicht davon ausgegangen werden, dass die Blockchain-Technologie bestehende Registersysteme (zB ZMR oder Firmenbuch) in ihrer Grundstruktur ersetzt.

[49] § 29 FBG.

[50] Die Frist zur Umsetzung ist mit 09.05.2018 bereits abgelaufen. Zum NISG besteht zum Zeitpunkt dieses Exposés lediglich ein Ministerialentwurf.

zur Gewährleistung der NIS[51] zu treffen".[52] Zur Beantwortung der Forschungsfrage wird sich das Dissertationsvorhaben insbesondere mit den folgenden Detailfragen beschäftigen:

(i) Ist die Bundesrechenzentrum GmbH (Betreiber der Firmenbuchdatenbank) oder das Bundesministerium für Inneres (Betreiber des ZMR) von dem NISG erfasst und wenn ja, welche Pflichten sind damit verbunden?

(ii) Fällt die Blockchain-Technologie unter dem im NISG geprägten Begriff "dem Stand der Technik entsprechende Sicherheitsvorkehrungen"?

(iii) Bietet das NISG eine ausreichende gesetzliche Grundlage um die Struktur der Firmenbuchdatenbank und/oder des ZMR durch den Einsatz der Blockchain-Technologie zu verändern?

Das Dissertationsvorhaben wird bei Auslegung des NISG zur Beantwortung der obenstehenden Fragen auch die Anwendbarkeit und die Implikationen des Staatsziels zur umfassenden Landesverteidigung gemäß Artikel 9a B-VG (insbesondere im Hinblick auf die zivile Landesverteidigung) berücksichtigen.

2.2 Zieht der Einsatz der Blockchain-Technologie in der Firmenbuchdatenbank und im ZMR datenschutzrechtliche Konsequenzen nach sich?

Mit dieser Forschungsfrage sollen die datenschutzrechtlichen Auswirkungen behandelt werden, die durch das Abspeichern von in der Firmenbuchdatenbank und im ZMR enthaltenen Daten als kodierte (und damit verschlüsselte) Standardwerte (Hashwerte) in eine Blockchain ausgelöst werden könnten. Hierzu müssen sowohl die Bestimmungen der DSGVO[53] und des DSG[54] im Zusammenhang mit Artikel 8 Abs 2 EMRK geprüft werden.

Aus datenschutzrechtlicher Sicht muss zwischen dem Firmenbuch und dem ZMR unterschieden werden:

<u>Firmenbuch</u>

Die Firmenbuchdatenbank enthält lediglich Daten juristischer Personen. Diese sind vom Schutzbereich der DSGVO und den einfachgesetzlichen Regelungen des DSG

[51] 78/ME XXVI. GP, § 3 Z 2: ""*Netz- und Informationssystemssicherheit": die Fähigkeit von Netz- und Informationssystemen, Sicherheitsvorfällen vorzubeugen, diese abzuwehren und zu beseitigen."*.

[52] 78/ME XXVI. GP, §§ 15 Abs. 1, 18 Abs. 1 und 19 Abs. 1.

[53] Verordnung (EU) 2016/679.

[54] Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG), BGBl I 165/1999 idF I 24/2018.

nicht erfasst. Lediglich das Grundrecht auf Datenschutz gemäß Artikel 1 DSG – welches nicht von der DSGVO im Sinne des Anwendungsvorrangs verdrängt wird[55] – ist weiterhin als Jedermannsrecht konzipiert und schützt damit auch juristische Personen. Allgemein verfügbare Daten, wie die im Firmenbuch ersichtlichen Informationen[56], sind allerdings nicht vom Grundrecht auf Datenschutz geschützt. Die Kodierung und Speicherung der in der Firmenbuchdatenbank enthaltenen Daten von juristischen Personen wird demnach wohl kein Eingriff in das Grundrecht auf Datenschutz sein und, mangels Anwendbarkeit von DSGVO und der einfachgesetzlichen Bestimmungen des DSG, auch keine sonstigen datenschutzrechtlichen Konsequenzen nach sich ziehen.

ZMR

Im Vergleich zum Firmenbuch, sind die datenschutzrechtlichen Vorzeichen für das ZMR andere: es werden Daten von natürlichen Personen gespeichert wodurch die DSGVO und die (verfassungs- und einfachgesetzlichen) Bestimmungen des DSG anwendbar sein könnten. Zur Prüfung der Anwendbarkeit der besagten Bestimmungen soll im Dissertationsvorhaben insbesondere beurteilt werden (i) ob es sich bei Hashwerten um "personenbezogene Daten" im Sinne von Artikel 4 Z 1 DSGVO handelt und, falls ja, ob die personenbezogenen Daten im Sinne von Artikel 4 Z 2 DSGVO verarbeitet werden, und (ii) wer "Verantwortlicher" im Sinne von Artikel 4 Z 7 DSGVO ist[57]. Parallel dazu soll geprüft werden ob das Grundrecht auf Datenschutz gemäß Artikel 1 DSG zur Anwendung gelangt. Hierzu ist es – neben der Tatsache, dass personenbezogene Daten betroffen sein müssen – entscheidend ob es sich beim ZMR um ein öffentliches Register handelt und die darin enthaltenen Daten als "allgemein zugängliche Daten" gemäß Artikel 1 Abs 1 DSG zu qualifizieren sind.

Sollte die DSGVO und das DSG auf den Sachverhalt anwendbar sein, wird im Dissertationsvorhaben auf die Voraussetzungen zur rechtmäßigen Datenverarbeitung durch eine Behörde eingegangen werden. Dabei werden vor allem die folgenden Fragen in den Fokus rücken[58]:

- Reicht es wenn die Verarbeitung im öffentlichen Interesse erfolgt?
- Muss eine konkrete gesetzliche Grundlage bestehen?
- Muss die Verarbeitung aus den in Artikel 8 Abs 2 EMRK genannten Gründen erforderlich sein?
- Welche Auswirkung hat die unveränderliche Grundstruktur der Blockchain-technologie auf die Betroffenenrechte der DSGVO und des DSG?

[55] *Anderl/Hörlsberger/Müller*, Kein einfachgesetzlicher Schutz für Daten juristischer Personen, ÖJZ 2018/3 (14).

[56] *Dohr/Pollirer/Weiss/Knyrim*, DSG § 1 Rz 8.

[57] Vgl hierzu § 16 Abs 1 MeldeG: "*Die Meldebehörden sind als gemeinsam Verantwortliche gemäß Art. 4 Z 7 in Verbindung mit Art. 26 Abs. 1 DSGVO ermächtigt […] .*".

[58] Vgl hierzu *Gerhartl*, Datenverarbeitung durch Behörden, ecolex 2018, 860.

2.3 Ist E-Voting in Österreich auf Blockchain-Basis im Hinblick auf den aktuellen verfassungsgesetzlichen Rahmen möglich?

Der Bericht Cyber Sicherheit 2018, der vom Bundeskanzleramt, dem Bundesministerium für Inneres, dem Bundesministerium für Landesverteidigung und dem Bundesministerium für Europa, Integration und Äußeres erstellt worden ist, enthält einen Lagebericht zur Cyber Sicherheit auf operativer Ebene.[59] Unter der Überschrift "Wahlen im Fokus" wird darauf hingewiesen, dass im deutschen Wahlsystem (speziell bei der Übermittlung von Wahlergebnissen an die übergeordneten Wahlbehörden) massive Sicherheitslücken bestehen. Eine Manipulation sei demnach denkbar.

Obwohl der Bericht Cyber Sicherheit 2018 (wohl auch aus politischen Gründen) versichert, dass eine solche Sicherheitslücke im österreichischen Wahlsystem nicht bestehe, bleibt ein fahler Beigeschmack im Hinblick auf potentielle Risiken bestehen. Neben möglichen Cyber-Risiken, ist insbesondere die Benutzerfreundlichkeit und die damit zusammenhängende Steigerung der Wahlbeteiligung die treibende Kraft für aufkeimende Forderungen nach E-Votings in Österreich. International wird insbesondere die Blockchain-Technologie als Schlüsseltechnologie zur Einhaltung der Wahlgrundsätze und zur Bewerkstelligung einer sicheren, transparenten und benutzerfreundlichen Wahl gesehen.[60] Scheiterte der einzige E-Voting-Versuch Österreichs[61] im Jahr 2009 noch an technischen und organisatorischen Unzulänglichkeiten[62], könnte ein zweiter Versuch mit Hilfe der Blockchain-Technologie im Zusammenspiel mit dem am 01.01.2018 eingeführten zentralen Wählerregister[63] Erfolg haben.

Zur verfassungsmäßigen Zulässigkeit soll im Dissertationsvorhaben geklärt werden, ob ein E-Voting auf Blockchain-Basis mit den Wahlrechtsgrundsätzen des B-VG vereinbar ist. Sollte E-Voting gegen einen verfassungsmäßigen Wahlgrundsatz verstoßen, werden erforderliche Verfassungsänderungen zur Umsetzung des E-Votings wissenschaftlich diskutiert werden. Weiters wird zu prüfen sein, inwieweit E-Voting

---

[59] Bericht Cyber Sicherheit 2018, https://www.bundeskanzleramt.gv.at/documents/131008/780563/Cybersicherheit_Bericht2018/769cb7b7-614c-49d8-8055-068d2f36009c (29.01.2019).

[60] *Hjalmarsson/Hreidarsson*, Blockchain-Based E-Voting System, https://skemman.is/bitstream/1946/31161/1/Research-Paper-BBEVS.pdf (30.01.2019); https://hackernoon.com/how-blockchain-will-make-electronic-voting-more-secure-fba15d752bee (30.01.2019); *Kshetri/Voas*, Blockchain-Enabled E-Voting, IEEE Software 35/4 2018 95-99.

[61] Österreichische Hochschülerinnen- und Hochschülerschaftswahlen 2009.

[62] VfGH 13.12.2011, V85/11 ua: Die Wahl wurde "*mangels hinreichender Determinierung des Handelns der Wahlkommission und wegen Fehlens einer Möglichkeit der Kontrolle der Einhaltung der bei der Stimmabgabe einzuhaltenden Grundsätze.*" aufgehoben.

[63] Wahlrechtsänderungsgesetz 2017, BGBl I Nr. 106/2016.

mit der in Artikel 141 B-VG vorgesehenen Möglichkeit zur nachträglichen Wahlanfechtung[64] und der verfassungsrechtlichen Zuständigkeit der Wahlbehörden[65] vereinbar ist.

2.4 In welchem verfassungsrechtlichen Rahmen kann die Blockchain-Technologie für E-Zustellungen[66] eingesetzt werden?

Die Forschungslandschaft zum Thema Blockchain und E-Government beschäftigt sich intensiv mit dem Thema E-Zustellung. So hat bereits die Wirtschaftskammer Österreich in ihrem Arbeitskreis "E-Zustellung" einen Use Case für Blockchain-basierte E-Zustellungen entwickelt und in einem Prototyp verwirklicht. Der Use Case soll den Prozess des Zustellnachweises (insbesondere der Verständigungen über die Zustellung) mit Hilfe der Blockchain-Technologie und Smart Contracts automatisieren.[67] Dabei sollen Informationen über die erfolgten Verständigungen über die Zustellung an die elektronische Adresse des Empfängers sowie die Metadaten des Dokuments auf der Blockchain gespeichert und jederzeit transparent vom Empfänger nachprüfbar sein. Einen Schritt weitergedacht sind Lösungen denkbar durch die der Zustelldienst komplett durch ein Blockchain-basiertes System mit Smart Contracts ersetzt werden könnte. Durch Änderungen des Zustellgesetzes und des Gerichtsorganisationsgesetzes könnte ein solcher Use-Case für behördliche bzw gerichtliche Zustellungen einfachgesetzlich umgesetzt werden. Die Grenze wird – wie bei allen einfachgesetzlichen Vorschriften – vom Verfassungsrecht gezogen. Im Dissertationsvorhaben werden zur Beurteilung der verfassungsrechtlichen Grenzen vor allem das Brief- und Fernmeldegeheimnis (Artikel 10 und Artikel 10a STGG), der Gleichheitssatz und das Diskriminierungsverbot sowie das Grundrecht auf Datenschutz als Grenzpfeiler identifiziert und im Lichte der möglichen Anwendungen der Blockchain-Technologie in der E-Zustellung geprüft werden.

[64] Vgl hierzu *Hofer*, E-Voting in Österreich, 19, http://webopac.fh-linz.at/dokumente/Bachelorarbeit_HoferF.pdf (30.01.2019).

[65] Artikel 26a Abs 1 B-VG; insbesondere hinsichtlich der Stimmauszählung und Leitung der Wahl.

[66] Im Sinne des § 35 Zustellgesetz.

[67] https://www.wko.at/service/netzwerke/blockchain-anwendungen-fuer-die-e-zustellung.html (30.01.2019).

3 Vorläufiges Inhaltsverzeichnis der Dissertation

1 Einleitung und Themengebiet

1.1 E-Government und Blockchain

1.1.1 E-Government in Österreich

1.1.2 Einführung in die Blockchain-Technologie

1.1.3 Einsatz der Blockchain-Technologie im E-Government

1.2 Aufbau der Dissertation

1.3 Forschungsfragen

2 Firmenbuch und ZMR

2.1 Rechtsrahmen

2.2 Vorfrage: Gibt es bereits einen ausreichenden gesetzlichen Rahmen im Lichte von Artikel 18 B-VG?

2.3 Erste Forschungsfrage: NIS-Richtlinie und NISG

2.3.1 Wer wird vom NISG verpflichtet?

2.3.2 Ist Blockchain-Technologie vom NISG erfasst?

2.3.3 Das NISG als gesetzliche Grundlage für einen Blockchain-Einsatz?

3 Datenschutzrechtliche Konsequenzen

3.1 Einleitendes zur zweiten Forschungsfrage

3.2 Firmenbuch

3.3 ZMR

3.3.1 Personenbezogene Daten

3.3.2 Verarbeitung

3.3.3 Verantwortliche

3.3.4 ZMR – ein öffentliches Register?

3.4 Verarbeitung im öffentlichen Interesse?

4 Vorläufiges Literaturverzeichnis

Aufsätze

Anderl/Hörslberger/Müller, Kein einfachgesetzlicher Schutz für Daten juristischer Personen, ÖJZ 2018/3.

Anderl/Tlapak, Warum Namen bei Türklingeln stehen dürfen, Die Presse 2018/43/01.

Blocher, The next big thing: Blockchain – Bitcoin – Smart Contracts, AnwBl (dt) 8+9/2016.

Böszörmenyi/Leissler, Unternehmensinterne Informationen: Wo endet der Datenschutz?, ecolex 2018, 789.

Buchleitner/Rabl, Blockchain und Smart Contracts: Revolution oder alter Wein im digitalen Schlauch, ecolex 2017, 4.

Ehrke-Rabel/Eisenberger/Hödl/Pachinger/Schneider, Kryptowährungen, Blockchain und Smart Contracts: Risiken und Chancen für den Staat (Teil I), jusIT 2017, 87.

Ehrke-Rabel/Eisenberger/Hödl/Pachinger/Schneider, Kryptowährungen, Blockchain und Smart Contracts: Risiken und Chancen für den Staat (Teil II), jusIT 2017, 129.

Freitag, Die Blockchain-Technologie. Nur ein Hype oder doch mehr?, CFOaktuell 2018, 59.

Gerhartl, Datenverarbeitung durch Behörden, ecolex 2018, 860.

Goby/Weichsel, Zur Verfassungskonformität von E-Voting bei den ÖH-Wahlen 2009, JAP 2009/2010/2.

Gorzala/Hanzl, Blockchain-Technologie und Datenschutzgrundverordnung – Anwendungsfragen, RdW 2018, 485.

Haimberger/Geuer, Anonymisierende Wirkung der Pseudonymisierung, Dako 2018/33.

Jakubek/Panic, Das Zusammenspiel zwischen der DSGVO und der Bitcoin Blockchain, MR 2018, 255.

Kaulartz/*Heckmann*, Smart Contracts – Anwendungen der Blockchain-Technologie, CR 9/2016.

Klaushofer, Cyber Security und der Schutz kritischer Infrastrukturen – eine Herausforderung für die Rechtsordnung, Journal für Rechtspolitik 23, 330-342 (2015).

Kreuzer, Was ist eine Blockchain?, CFOaktuell 2017, 109.

Lachmayer, Elektronische Schulverwaltung und Datenschutz, S&R 1/2015/18.

Lehner, Zustellung durch Zustelldienst: "E-Zustellung" (§§ 28 ff ZustG), ÖRPfl 2016 H1, 21.

Lichtenstrasser/Mosing/Otto, Wireless LAN – Drahtlose Schnittstelle für Datenmissbrauch?, ÖJZ 2003/14.

Morscher/Waitz, Zum Schutz des Briefgeheimnisses, JBl 2008, 424.

Müller, Bitcoin, Blockchain und Smart Contracts, ZfIR 17-18/2017.

Pesch/Böhme, Datenschutz trotz öffentlicher Blockchain? DuD 2017, 93.

Piska/Völkel, Blockchain und Kryptorecht: Regulierungs-Chance de lege lata und de lege ferenda, ZTR 2017, 97.

Poier, E-Voting – mehr als ein einmaliger Flop?, Jahrbuch Öffentliches Recht 2013, 139.

Schrey/*Thalhofer*, Rechtliches zur Blockchain, NJW 20/2017.

Seeber/*Schweiger*/*Schachner*, Immobilientransaktionen über die Blockchain, immolex 2018, 38.

Smets/*Kapeller*, Smart Contracts: Vertragsabschluss und Haftung, ÖJZ 2018/39.

Spitzbart/Geuer, Zielgerichtete Werbung für Kunden in sozialen Netzwerken, Dako 2017/21.

Stein/Wenda, Die Wahlrechtsreform 2007, SIAK-Journal 2007 H 4, 61.

Stober, Sicherheit als offene Querschnittsaufgabe: Die deutsche Perspektive unter Berücksichtigung von Sicherheitsmärkten, SIAK-Journal 2014 H 2, 68.

Wessely, Das Fernmeldegeheimnis – ein unbekanntes Grundrecht?, ÖJZ 1999, 491.

Wiederin, Das Erkenntnis über die Stichwahl zum Bundespräsidenten: Eine verfassungsrechtliche Nachlese, Jahrbuch Öffentliches Recht 2017, 9.

Wiefling/Iacono/Sandbrink, Anwendung der Blockchain außerhalb von Geldwährungen, DuD 2017, 482.

Wilsch, die Blockchain-Technologie aus der Sicht des deutschen Grundbuchrechts, DNotZ 2017, 761.

Monografien/Sammelwerke

Forgó/Zöchling-Jud, Das Vertragsrecht des ABGB auf dem Prüfstand: Überlegungen im digitalen Zeitalter, 20. ÖJT Band II/1.

Kindler in *Schnauder (Hrsg)*, Digitalisierung im Gesellschaftsrecht (2017).

Raffling/Schock (Hrsg), Digitale Wirtschaft und Industrie 4.0 (2018).

Kommentare

Bumberger/Schmid, Praxiskommentar zum Zustellgesetz (2018).

Kneihs/Lienbacher (*Hrsg*), Rill-Schäffler-Kommentar Bundesverfassungsrecht[21] (2018).

Knyrim, DatKomm (2018).

Mayer/Muzak, Bundesverfassungsrecht[5] (2015).

Pollirer/Weiss/Kyrim/Haidinger, DSGVO (2017).

Internetwerke

Digitales Österreich, Behörden im Netz: Das österreichische E-Government ABC, https://www.digitales.oesterreich.gv.at/documents/22124/30428/E-Government-ABC.pdf.

Fraunhofer, Blockchain und Smart Contracts, https://www.fraunhofer.de/content/dam/zv/de/forschung/artikel/2017/Fraunhofer-Positionspapier_Blockchain-und-Smart-Contracts_v151.pdf.

Hjalmarsson/Hreidarsson, Blockchain-Based E-Voting System, https://skemman.is/bitstream/1946/31161/1/Research-Paper-BBEVS.pdf.

Hofer, E-Voting in Österreich, 19, http://webopac.fh-linz.at/dokumente/Bachelorarbeit_HoferF.pdf.

Kompetenzzentrum Öffentliche IT, Mythos Blockchain: Herausforderungen für den öffentlichen Sektor, https://www.oeffentliche-it.de/documents/10181/14412/Mythos+Blockchain+-+Herausforderung+f%C3%BCr+den+%C3%96ffentlichen+Sektor.

Linklaters, Smart Contracts and Distributed Ledger – A Legal Perspective, https://www.isda.org/a/6EKDE/smart-contracts-and-distributed-ledger-a-legal-perspective.pdf.

Müller/Windisch, E-Identity-Initiativen – Der europäische Weg, https://asquared.company/public/asquared-blog_post_de_2018-01-22_e-identity-initiativen_der-europ%C3%A4ische-weg.pdf.

Ollrom, Auswirkungen von Blockchains auf die E-Government-Services des Bundes: Evolution oder Revolution, http://pub.fh-campuswien.ac.at/obvfcwhsacc/download/pdf/2063683?originalFilename=true.

Perkins Coie, Legal Aspects of Smart Contract Applications, https://www.virtualcurrencyreport.com/wp-content/uploads/sites/13/2017/05/Perkins-Coie-LLP-Legal-Aspects-of-Smart-Contracts-Applications.pdf.

Spancken/Hellenkamp/Brown/Thiel, Kryptowährungen und Smart Contracts, https://www.hb.fh-muenster.de/opus4/frontdoor/deliver/index/docId/920/file/FuE_Kryptowaehrungen_und_Smart_Contracts_Abschlussbericht.pdf.

5 Zeitplan

Das Dissertationsvorhaben soll im 2. Quartal 2020 fertiggestellt werden. Der genaue Zeitplan erfolgt in Absprache mit dem Dissertationsbetreuer.