Forschungsprojekts „STORE&GO" (Projektnummer: 691797 (https://www.storeandgo.info/) sowie der im Rahmen der vom Klima- und Energiefonds geförderten Vorzeigeregion WIVA P&G durchgeführten Projekte „UpHy I" (Projektnummer: 868835), „Renewable Gasfield" (Projektnummer: 868849) und „HyTruck" (Projektnummer: 868790).

> MAG.ª ARGJENTA VESELI

Abteilung Energierecht, Energieinstitut an der JKU Linz,
E-Mail: veseli@energieinstitut-linz.at,
Web: http://www.energieinstitut-linz.at

> DR. ROBERT TICHLER

Geschäftsführer des Energieinstituts an der JKU Linz,
E-Mail: tichler@energieinstitut-linz.at,
Web: http://www.energieinstitut-linz.at

> CHRISTIAN M. PISKA / SASCHA SMETS

Blockchain und neuartige kryptographische Verfahren: Der Schlüssel zu E-Votings in Österreich?

Die Corona-Krise macht die Forderung nach E-Votings in Österreich bei öffentlich-rechtlichen Wahlen wieder lauter. Halten aktuell verfügbare Technologien den rechtlichen Anforderungen an ein elektronisches Wahlsystem stand? Es wird Zeit, angestaubte E-Voting-Überlegungen in Österreich wieder aus der Schublade zu holen.

I. E-Voting? Kann man das überhaupt nochmal aufwärmen?

Man kennt es noch aus der Studienzeit: Ganz hinten im Kühlschrank oxidiert das verdächtig riechende Gulasch von letzter Woche. Essen sollte man es nicht, wegschmeißen will man es nicht. Mit jedem Magenknurrer nähert man sich dem Kühlschrank. Der Kopf sagt zunächst nein, der vom Hunger gebeugte Wille sagt schließlich ja. Das Bedauern kommt hinterher. Ein altbekannter Kampf zwischen Bedürfnis und Verstand, der seit dem bislang einzigen elektronischen Abstimmungsversuch bei den ÖH-Wahlen 2009 auch in puncto E-Votings[1] in der Öffentlichkeit und der juristischen Literaturlandschaft ausgetragen wird.

Das Bedürfnis nach einer sicheren, elektronischen Stimmabgabe wurde auch in jüngerer Vergangenheit wieder geweckt. So wies der Bericht Cyber Sicherheit 2018[2] auf massive Sicherheitslücken im analogen Wahlsystem Deutschlands hin. Auch in Österreich wurden spätestens mit dem Wahlkarten-Fiasko um die Bundespräsidentenwahl 2016 die Schwächen unseres Wahlsystems gnadenlos aufgedeckt.[3] Forderungen

1 Unter E-Voting wird die Stimmabgabe des Wählers im elektronischen Weg im Sinne einer Distanzwahl unter Nutzung des Internets verstanden. Siehe dazu *Weichsel*, E-Voting am Beispiel der ÖH-Wahlen 2009 (2017) 62 f.

2 Siehe dazu *Cyber Sicherheit Steuerungsgruppe (CSS)*, Bericht Cyber Sicherheit (2018) 7, abrufbar unter <https://www.bundeskanzleramt.gv.at/themen/cyber-sicherheit-egovernment.html> (Stand 30.03.2020). Der Cyber Bericht 2019 verweist auf den Cyber Bericht 2018, baut auf diesen auf und ergänzt ihn um neue Punkte (siehe *Cyber Sicherheit Steuerungsgruppe (CSS)*, Bericht Cyber Sicherheit (2019) 57 ff, abrufbar unter <https://www.bundeskanzleramt.gv.at/themen/cyber-sicherheit-egovernment/nis-buero.html> (Stand 30.03.2020). Die im Cyber Bericht 2018 beschriebenen Risiken haben daher weiterhin Bestand.

3 *Wiederin*, Das Erkenntnis über die Stichwahl zum Bundespräsidenten: Eine verfassungsrechtliche Nachlese, Jahrbuch Öffentliches Recht

nach E-Votings werden daher auch hierzulande immer lauter.[4] Mit ihnen wären demokratische Wahlen schließlich auch bei Ausgangsbeschränkungen denkbar.

Warum wurde der digitale Hunger also bis dato nicht gestillt? Liegt es am juristischen Verstand, der das metaphorische Gulasch weiter im Kühlschrank schmoren lässt? Mit Blick auf den bislang einzigen E-Voting-Versuch Österreichs bei den ÖH-Wahlen 2009 und dem daraus resultierenden Erkenntnis des VfGH (im Folgenden: E-Voting-Erkenntnis)[5] lässt sich die Frage mit einem klaren Ja beantworten. Um einer wiederholenden Beschreibung des E-Voting-Erkenntnisses zu entgehen, darf an dieser Stelle auf die reichhaltige, einschlägige Literatur verwiesen werden.[6] So viel sei allerdings festgehalten: Bislang konnte die Technik den vom VfGH in seinem E-Voting-Erkenntnis zum Ausdruck gebrachten Anforderungen an ein elektronisches Wahlverfahren nicht entsprechen. Die verfügbaren IT-Lösungen wiesen einfach nicht die erforderlichen Features auf.

Laut VfGH muss die Technik im Wesentlichen die folgenden drei Voraussetzungen erfüllen: (i) Das **geheime, persönliche und freie Wahlrecht** muss auf einem **Briefwahl-ähnlichen Niveau** geschützt werden; (ii) den WählerInnen ist zu jeder Zeit **Zugang zum Quellcode** des zur Anwendung kommenden Systems zu gewähren; und (iii) die **Wahlbehörden** müssen ihre Aufgaben (insbesondere die Kontrolle der Richtigkeit der Stimmabgaben) **ohne Sachverständige nachvollziehbar** ausüben können.[7] Ein Aufwärmen von E-Voting-Überlegungen in Österreich scheint daher erst in jenem Zeitpunkt sinnvoll, an dem die Technik den vom VfGH postulierten Herausforderungen gewachsen ist. Mit bekannten E-Voting-Systemen, die zentrale Datenbanken verwenden,[8] scheint dieser Zeitpunkt noch nicht gekommen zu sein.[9]

Das zeigt sich auch im internationalen Vergleich: dem in Estland verwendeten, zentralen E-Voting-System werden große Sicherheitslücken unterstellt.[10] Auch der bislang größte (zentrale) Schweizer E-Voting Probelauf ist als gescheitert anzusehen.[11] Ein neuer (dezentraler) E-Voting-Versuch im Schweizer Kanton Zug[12] zeigt jedoch, dass neue Technologien den rechtlichen Anforderungen des VfGH standhalten und somit bei näherer Betrachtung verfassungskonforme E-Votings in Österreich tatsächlich ermöglichen könnten.

II. Der E-Voting Use-Case auf dezentraler Basis

Im Schweizer Kanton Zug wurde ein E-Voting auf Blockchain[13]-Basis implementiert, welches modular aufgebaut ist und aus einzelnen Komponenten und Anwendungsschritten besteht. Es handelt sich daher um keinen einheitlichen, vollautomatisierten Prozess. Die technische Beschreibung der einzelnen Schritte zur elektronischen Stimmabgabe kann im einschlägigen Projektabschlussbericht der Stadt Zug nachgeschlagen werden.[14] Entscheidend sind folgende Eigenschaften des dort angewandten Systems:

Die WählerInnen identifizieren sich mit ihren digitalen Identitäten, die mit der Bürgerkarte bzw Handysignatur hierzulande zu vergleichen sind. Einziger Unterschied: die im Kanton Zug verwendete digitale ID wird dezentral auf der Ethereum-Blockchain verwaltet.[15] Die Identifikation erfolgt im Zuge der an die Wahlbehörde gestellten Anfrage auf Zusendung eines elektronischen Stimmzettels, die mit der digitalen Identität signiert wird. Danach prüft die Wahlbehörde die Identität und sendet der WählerIn den Stimmzettel zu.

Im Anschluss erfolgt die eigentliche Stimmabgabe. Der Use-Case setzt dabei auf das private und permissioned

(2017) 9 (23 ff). Vgl auch *Strejcek*, Wehrlos ums Wahlrecht umgefallen, Die Presse 2019/41/04, zur letzten NR-Wahl.

4 So etwa der Beitrag „Wählen mit Smartphone könnte sicherer sein als mit Stift und Zettel" von *Sommavilla*, abrufbar unter <https://www.derstandard.at/story/2000097743990/waehlen-mit-smartphone-koennte-sicherer-sein-als-mit-stift-und> (Stand 30.03.2020).

5 VfSlg 19.592/2011.

6 Siehe etwa *Poier*, E-Voting – mehr als ein einmaliger Flop?, Jahrbuch Öffentliches Recht (2013) 139; *Weichsel*, E-Voting (FN 1); *Goby/Weichsel*, Wählen per Mouse Click?, JAP 2009/2010, 17 ff.

7 Siehe FN 5.

8 I.e. ein Client-Server-System, bestehend aus einem zentralen Datenbankserver. Das Gegenteil: dezentrale Peer-2-Peer-Systeme mit mehreren Netzwerkknoten, wie etwa die Blockchain-Technologie.

9 Statt vieler *Poier*, E-Voting (FN 6) 139 f, 156.

10 Siehe dazu den Beitrag „These are the arguments that sank e-voting in Switzerland" von *Kuenzi*, abrufbar unter <https://www.swissinfo.ch/eng/e-voting_these-are-the-arguments-that-sank-e-voting-in-switzerland/45136608?> (Stand 30.03.2020).

11 Siehe dazu den Beitrag „Flaw reported in Switzerland's biggest e-voting system", abrufbar unter <https://www.swissinfo.ch/eng/politics/online-voting_flaw-reported-in-switzerland-s-biggest-e-voting-system/44522012> (Stand 30.03.2020).

12 Siehe dazu die „Auswertung der Blockchain-Konsultativabstimmung in der Stadt Zug", abrufbar unter <https://news.hslu.ch/wp-content/uploads/2019/02/eVoting-Stadt-Zug-Abschlussbericht-DE.docx> (Stand 30.03.2020).

13 Für eine technische Beschreibungen siehe etwa *Völkel*, Grundlagen der Blockchain-Technologie und virtuellen Währungen, in Piska/Völkel (Hg), Blockchain rules (2019) 1 (1 ff); *Fraunhofer*, Blockchain und Smart Contracts (2017) 10 f, abrufbar unter <https://www.fraunhofer.de/content/dam/zv/de/forschung/artikel/2017/Fraunhofer-Positionspapier_Blockchain-und-Smart-Contracts_v151.pdf> (Stand 30.03.2020).

14 Siehe FN 12.

15 Siehe FN 13.

Hyperledger-Fabric Blockchain-Protokoll.[16] Die Daten werden – im Gegensatz zur Ethereum- oder Bitcoin-Blockchain – lediglich in ausgewählten Rechenzentren verarbeitet.[17]

Jede WählerIn erhält mit ihrem Stimmzettel ein kryptographisches Schlüsselpaar, bestehend aus einem privaten und einem öffentlichen Schlüssel. Mit dem privaten Schlüssel signiert und verschlüsselt die WählerIn ihre Stimmabgabe. Dabei wird ein homomorphes Verschlüsselungssystem angewandt, wodurch Daten trotz aufrechter Verschlüsselung berechnet werden können (i.e. die Stimmenanzahl für eine Partei kann berechnet werden, ohne einzelne Stimmabgaben zu entschlüsseln).[18] Die ausgefüllten elektronischen Stimmzettel werden an die Hyperledger-Fabric-Blockchain kommuniziert und bis zur Stimmauszählung dezentral verwahrt.

Durch die homomorphe Verschlüsselung kann die Wahlbehörde demnach die **Stimmen auszählen, ohne sie zu entschlüsseln**. Das Wahlergebnis wird sodann mit einem Zero-Knowledge-Beweis versehen.[19] Dadurch kann das Ergebnis durch die Wahlbehörde, die Gerichte und die einzelnen WählerInnen überprüft werden, ohne die Anonymität der Stimmabgabe aufzugeben. Im Gegensatz zur Briefwahl kann die einzelne WählerIn mit diesem Beweis auch das Schicksal ihrer eigenen Stimmabgabe nachverfolgen (also etwa ob die Stimme für die richtige Partei zur Auszählung gelangt ist). Die Technologie ist „Open Source". Dadurch kann jeder zu jeder Zeit den Quellcode des Systems einsehen. Darin liegt – laut dem Abschlussbericht der Stadt Zug – auch der größte Vorteil des angewandten, dezentralen Wahlsystems.[20]

III. Einhaltung der Wahlrechtsgrundsätze

Bei den ÖH-Wahlen 2009 kamen die verfassungsgesetzlichen Wahlrechtsgrundsätze nicht zur Anwendung, weil es sich um Wahlen von Organen der nichtterritorialen Selbstverwaltung handelte.[21] Allerdings enthielt § 34 HSG[22] einfachgesetzliche Wahlrechtsgrundsätze, die den verfassungsgesetzlichen Grundsätzen des Art 26 Abs 1 B-VG nachempfunden waren. Somit lassen sich die Aussagen des E-Voting-Erkenntnisses auch auf E-Votings umlegen, die auf Basis der verfassungsgesetzlichen Wahlrechtsgrundsätze stattfinden müssen.

Im E-Voting-Erkenntnis hat der VfGH klargestellt, dass E-Voting-Systeme die Einhaltung der Wahlrechtsgrundsätze auf einem Briefwahl-ähnlichen Niveau sicherstellen müssen. Dabei sind ausschließlich das freie, geheime und persönliche Wahlrecht betroffen. Die Einhaltung dieser Grundsätze wird bei der analogen Briefwahl mit einer eidesstaatlichen Erklärung der WählerIn gemäß Art 26 Abs 6 B-VG gewährleistet. Eine derartige eidesstaatliche Erklärung könnte technisch auch bei einem E-Voting umgesetzt werden (so auch bei den ÖH-Wahlen 2009 geschehen).[23]

Zusätzliche Möglichkeiten zur Sicherstellung der Wahlrechtsgrundsätze bieten die einzelnen technischen Komponenten des E-Voting-Systems am Beispiel des beschriebenen Use-Cases. Mit elektronischer Identifikation und speziellen Verschlüsselungstechniken können die Grundsätze des geheimen und persönlichen Wahlrechts, die wiederum der Einhaltung des freien Wahlrechts dienen,[24] zusätzlich abgesichert werden.

Das in der Schweiz umgesetzte E-Voting-System bietet allerdings noch einen besonderen Reibungspunkt mit dem geheimen Wahlrechtsgrundsatz: Die WählerInnen können das Schicksal der von ihnen abgegebenen Stimme nachverfolgen. Das Wahlverhalten wäre für die WählerInnen beweisbar. Versprechungen wahlwerbender Parteien bei Vorlage eines Beweises des Wahlverhaltens könnten für psychischen Druck bei der Stimmabgabe sorgen. Allerdings wären derartige Incentivierungen auch beim aktuellen, analogen Wahlsystem denkbar. Schließlich könnte die WählerIn ihr Wahlverhalten durch ein Foto dokumentieren und somit beweisen. Mit der Blockchain-Technologie

16 Vgl zu den unterschiedlichen Blockchain-Arten etwa *Raffling/Schock* (Hg), Digitale Wirtschaft und Industrie 4.0 (2018) 167 ff oder *Piska/Wagner*, Zukunftstechnologie Blockchain und wie man den Stolperstein DSGVO vermeiden kann, ZTR 2018, 195.

17 Viele kritisieren dabei, dass die eigentliche anarchistisch-romantische Grundprämisse der Blockchain-Technologie, nämlich die totale Dezentralität, damit torpediert werden würde (etwa der Beitrag „These are the arguments that sank e-voting in Switzerland" von *Kuenzi*, abrufbar unter <https://www.swissinfo.ch/eng/e-voting_these-are-the-arguments-that-sank-e-voting-in-switzerland/45136608?> [Stand 30.03.2020]).

18 Siehe hierzu *European Parliamentary Research Service (EPRS)*, Blockchain and the General Data Protection Regulation, PE 634.445 (2019) 33 f, abrufbar unter <https://www.europarl.europa.eu/stoa/en/document/EPRS_STU(2019)634445> (Stand 30.03.2020); *Sadeghi/Schneider*, Verschlüsselt Rechnen: Sichere Verarbeitung Verschlüsselter Medizinischer Daten am Beispiel der Klassifikation von EKG Daten (2010) 3 f, abrufbar unter <https://encrypto.de/papers/SS10.pdf> (Stand 30.03.2020).

19 *EPRS*, Blockchain and the General Data Protection Regulation, PE 634.445 (2019) 32 f, abrufbar unter <https://www.europarl.europa.eu/stoa/en/document/EPRS_STU(2019)634445> (Stand 30.03.2020); „Was ist Zero-Knowledge-Verschlüsselung" von *Lám*, abrufbar unter <https://tresorit.com/blog/zero-knowledge-verschlusselung/> (Stand 30.03.2020).

20 Siehe FN 12.

21 Siehe FN 5.

22 Bundesgesetz über die Vertretung der Studierenden (Hochschülerinnen- und Hochschülerschaftsgesetz 1998 – HSG 1998), BGBl I 22/1999 idF BGBl I 47/2007.

23 Bspw mit einem Häkchen, das mit der qualifizierten, digitalen Signatur der WählerIn signiert wird.

24 Vgl dazu *Schreiner*, Art 26 B-VG, in Kneihs/Lienbacher (Hg), Rill-Schäffer-Kommentar Bundesverfassungsrecht (1. Lfg, 2001) Rz 54 und VfSlg 3843/1960.

würde die Beweisbarkeit wohl lediglich bereits im System liegen. Lehre und Rsp sehen in der nachträglichen Veröffentlichung des Wahlverhaltens durch die WählerIn selbst allerdings keinen relevanten Verstoß gegen das geheime Wahlrecht.[25]

Will der Gesetzgeber dieses Risiko dennoch vermeiden, könnte er sich an den ÖH-Wahlen 2009 orientieren. Damals konnte die WählerIn lediglich die Registrierung ihrer Stimme nachverfolgen. Wem die Stimme tatsächlich zugezählt wurde, konnte nicht von der WählerIn überprüft werden.

Ob nun tatsächlich ein Briefwahl-ähnliches Sicherheitsniveau gewährleistet werden kann, wird in der Praxis von einer Vielzahl von Faktoren abhängen: Wurden das Blockchain-Protokoll, die verwendeten Smart Contracts und die Front-End Schnittstellen fehlerfrei codiert? Sind die Verschlüsselungstechniken zukünftig resistent gegen die Rechenleistung von Quantencomputern? Hält die Open Source Technologie Stresstests durch Technik-Audits und allfälligen Prüfungen von Bestätigungsstellen iSd § 7 Abs 3 SVG stand?[26] Nur wenn dies der Fall ist, könnte das rechtspolitische Pendel zukünftig in Richtung von E-Votings ausschlagen.

IV. Offenlegung des Quellcodes

Die Datenverarbeitung beim Use-Case war aufgrund der „Open Source"-Eigenschaft der verwendeten Blockchain-Protokolle transparent und nachvollziehbar. Das heißt, der Quellcode war für jedermann zu jeder Zeit einsehbar. Während die Quellcodes zentraler E-Voting-Systeme, wie jenes der ÖH-Wahlen 2009, aus Sicherheitsgründen nicht der Öffentlichkeit zugänglich gemacht werden, wäre eine Veröffentlichung bei dezentralen Systemen aufgrund der ungleich höheren Ressourcen (insb Rechenleistungen), die für Cyber-Angriffe notwendig wären, möglich.

V. Richtigkeitskontrolle ohne Sachverständige

Wahlbehörden müssen bei E-Votings ihre Pflichten (insbesondere die Richtigkeitskontrolle der Stimmabgabe) ohne technische Sachverständige nachvollziehbar ausüben können. Einige sehen darin eine Verunmöglichung von E-Votings in Österreich;[27] andere eine Anleitung zur rechtlich-konformen technischen Ausgestaltung solcher Systeme.[28]

Man könnte es am Beispiel des Schweizer Use-Cases sogar noch rosaroter sehen: Die einzelnen Software-Komponenten könnten die Pflichterfüllung der Wahlbehörden sogar erleichtern. Die Identität kann mit der Bürgerkartenfunktion geprüft werden, die Echtheit der Stimmabgabe ist mit der Signierung durch den privaten Schlüssel nachvollziehbar und durch den Zero-Knowledge Beweis und homomorphe Verschlüsselungen kann das Stimmergebnis durch einfache Additionsfunktionen nachgerechnet werden. Nüchtern betrachtet hängt alles bloß von einer entsprechenden Programmierung der Systeme ab, die den Wahlbehörden eine selbständige Bedienung ermöglichen müssen.

Wie *Poier* bereits zutreffend festgestellt hat, darf man dem VfGH auch nicht unterstellen E-Votings per se verunmöglichen zu wollen.[29] Es sollte daher ausreichen, dass die Wahlbehörde ihre Aufgaben ohne Sachverständige ausüben kann. Dabei kann nicht verlangt werden, dass jedes einzelne Mitglied der Wahlbehörde den dahinterliegenden Quellcode bzw das kryptographische Verfahren verstehen muss. Soweit geht man bei der verfassungsgesetzlich vorgesehenen Briefwahl schließlich auch nicht. Die Wahlbehörden müssen den Quellcode der Software, mit dem die Wahlkarte elektronisch beantragt werden kann,[30] auch nicht ohne Sachverständige verstehen und auslegen können.

Tatsächlich zeigen die Postulate des VfGH nur, dass E-Votings nicht auf vollautomatisierte, einheitliche Systeme gestützt werden sollten. Ein System, das der Wahlbehörde ausschließlich das fertige Wahlergebnis liefert, scheint nicht ohne Sachverständige nachvollziehbar zu sein. Laut *Poier* kann der Anforderung nur entsprochen werden, wenn das Wahlsystem in einzelne, unabhängige Schritte aufgeteilt wird.[31] Der geschilderte Use-Case zeigt in diesem Zusammenhang die Blockchain-basierte Richtung.

VI. Aufgewärmt oder doch frisch gekocht?

Das Gesagte verdeutlicht: Ein Knopfdruck auf die Mikrowelle wird nicht ausreichen, um E-Voting-Gedanken wieder aufzuwärmen. So lange man dasselbe techno-

25 *G. Holzinger/K. Holzinger*, Art 26 Abs 1 B-VG, in Korinek/Holoubek (Hg), Österreichisches Bundesverfassungsrecht (3. Lfg, 2000) Rz 57 mwN; siehe auch VfSlg 5229/1966 zur öffentlichen Stimmabgabe.

26 So kann die Einhaltung des Standes der Technik bspw durch das Zentrum für sichere Informationstechnologie – Austria (A-SIT) bescheinigt werden. So ist das auch bei den ÖH-Wahlen 2009 geschehen. Vgl dazu *Weichsel*, E-Voting (FN 1) 76 und *Lehner*, Die Wahlen zur Österreichischen Hochschülerinnen- und Hochschülerschaft (2010) 97.

27 So etwa *Weichsel*, E-Voting (FN 1) 115.

28 Vgl *Poier*, E-Voting (FN 6) 139.

29 Siehe FN 28.

30 Vgl § 39 Abs 1 NRWO.

31 Siehe FN 28.

logische Rezept wie bei den gescheiterten ÖH-Wahlen 2009 verwendet, wird man spätestens beim verfassungsgerichtlichen Verdauungsprozess im Rahmen eines Gesetzes- bzw Verordnungsprüfungsverfahrens ein böses Erwachen erleben. Es braucht neue Zutaten: Neuartige Kryptographische Verfahren und modularaufgebaute (dezentrale) Systeme. Damit das neue Rezept dem VfGH schmeckt und von den Wahlbehörden und den WählerInnen nachgekocht werden kann, muss wie eben gezeigt bei zukünftigen E-Voting-Versuchen auf disruptive Technologien (zB Blockchain) gesetzt werden.

Man darf sich dabei allerdings nicht nur auf die zum Einsatz kommende Technologie verlassen. Auch legistisch muss das E-Voting auf einwandfreie Beine gestellt werden. Das fängt bei der benötigten verfassungsgesetzlichen E-Voting-Ausnahmebestimmung für Wahlen, bei denen die verfassungsrechtlichen Wahlrechtsgrundsätze zur Anwendung kommen, an und endet bei der entsprechenden einfachgesetzlichen Ausgestaltung. Insbesondere die einfachgesetzlichen Bestimmungen und etwaige Verordnungen müssen hierbei eine Vielzahl von inhaltlichen Kriterien erfüllen. Dazu zählt etwa die hinreichend determinierte Beschreibung des zum Einsatz kommenden technischen Systems.[32]

Die betreffenden Bestimmungen müssen außerdem Antworten auf Fragen des Übereilungsschutzes, der Datenspeicherung, der Maßnahmen bei technischem Gebrechen und der organisatorischen und technischen Barrieren zur doppelten Stimmabgabe geben.[33] Falls die verwendeten öffentlichen Schlüssel als personenbezogene Daten einzuordnen wären, müssten darüber hinaus auch datenschutzrechtliche Bestimmungen beachtet werden.[34]

Mit der passenden Technik allein werden E-Votings in Österreich daher nicht zum Selbstläufer. Es erfordert eine perfekt ausbalancierte legistische und technische Komposition um den Erfordernissen des VfGH gerecht zu werden. Ein sensibles Projekt, dem auch die ÖVP/FPÖ-Koalition aus dem Weg gegangen ist.[35] Die rechtspolitische Vorsicht, mit der E-Votings in Österreich behandelt werden, ist auch mit den (teils unkontrollierbaren) Risken von elektronischen Wahlsystemen verbunden. Man mag hierbei nur an manipulierte Videos denken, mit denen angebliche Fehler des Wahlsystems in einem Video dokumentiert und veröffentlicht werden.[36] Große Vertrauensverluste wären die Folge. Ebenso könnten bekannte Wahlbetrugsarten an Skalierbarkeit dazugewinnen.[37]

Trotzdem: Je näher E-Votings durch neuartige technische Verfahren an die verfassungskonforme Vorstellung des VfGH gerückt werden, desto weniger werden sich die Parteien den aufkeimenden Forderungen nach E-Votings entziehen können. Dass die Zeit für E-Votings bald gekommen sein könnte, zeigt der beschriebene Use-Case.

VII. Fazit

Neue technologische Möglichkeiten lassen E-Votings in Österreich wieder juristisch machbar erscheinen. Ein in der Schweiz umgesetzter Use-Case auf Basis der Blockchain-Technologie zeigt den Weg, mit dem elektronische Wahlsysteme in Österreich den vom VfGH im E-Voting-Erkenntnis zu den ÖH-Wahlen 2009 postulierten Anforderungen entsprechen könnten.

> DR. CHRISTIAN M. PISKA

Ao. Univ.-Prof. für öffentliches Recht am Juridicum Wien, 1010 Wien, Schottenbastei 10-16. E-Mail: christian.piska@univie.ac.at, Web: staatsrecht.univie.ac.at.

> MAG. SASCHA SMETS

Projektmanager M&A und Venture Capital bei der Österreichischen Post AG, 1030 Wien, Rochusplatz 1. E-Mail: sascha.smets@post.at, Web: www.post.at.

32 Siehe FN 5.

33 Die genannten Kriterien ergeben sich aus einer Zusammenschau der NRWO, Art 141 B-VG und dem E-Voting-Erkenntnis.

34 Vgl zur datenschutzrechtlichen Einordnung der öffentlichen Schlüssel etwa *Piska/Bierbauer*, Datenschutzrechtliche Dimensionen der Blockchain-Technologie, in Piska/Völkel (Hg), Blockchain rules (2019) 164 (181).

35 Siehe dazu etwa https://www.derstandard.at/story/2000097743990/waehlen-mit-smartphone-koennte-sicherer-sein-als-mit-stift-und (29.04.2020)..

36 Zu denken ist hier auch an Anwendungen der *Deepfake*-Technik; vgl dazu „Deepfake" von Wikipedia, abrufbar unter <https://de.wikipedia.org/wiki/Deepfake> (Stand 30.03.2020).

37 Wie etwa das *Granny Farming*; siehe *Pratchett/Wingfield/Fairweather/Rogerson*, Balancing security and simplicity in e-voting. Towards an effective compromise?, in Mendez/Trechsel (Hg), The European Union and E-Voting (2004) 166 oder *Young*, International Election Principles (2010) 224.