Neue Zeitschrift für Verwaltungsrecht – Online-Aufsatz

In Zusammenarbeit mit der Neuen Juristischen Wochenschrift

Gegründet von Rechtsanwalt **Prof. Dr. Hermann Weber**, Schriftleiter von 1982–2001

Herausgegeben von **Prof. Dr. Christoph Brüning,** Präsident des SchlHLVerfG, Kiel – **Prof. Dr. Martin Burgi,** München – **Prof. Dr. Christian Calliess,** Berlin – **Dr. Josef Christ,** Richter des BVerfG a. D., Karlsruhe – **Dr. Frank Fellenberg,** Rechtsanwalt, Berlin – **Prof. Dr. Andreas Heusch,** Präsident des VG, Düsseldorf – **Prof. Dr. Andrea Kießling,** Frankfurt a. M. – **Prof. Dr. Christoph Külpmann,** Vorsitzender Richter am BVerwG, Leipzig – **Prof. Dr. Thomas Mayen,** Rechtsanwalt, Bonn – **Prof. Dr. Hubert Meyer,** Geschäftsf. Vorstandsmitglied des Niedersächsischen Landkreistages a. D., Hannover – **Prof. Dr. Sabine Schlacke,** Greifswald – **Dr. Heribert Schmitz,** Ministerialrat a. D., Berlin – **Prof. Dr. Friedrich Schoch,** Freiburg – **Dr. Thomas Schröer,** Rechtsanwalt, Frankfurt a. M. – **Prof. Dr. Rudolf Streinz,** München – **Dr. Andrea Vetter,** Rechtsanwältin, Stuttgart – **Dr. Holger Wöckel,** Richter des BVerfG, Karlsruhe

Schriftleitung: Rechtsanwalt **Dr. Johannes Heuschmid,** Beethovenstraße 7 b, 60325 Frankfurt a. M.

3 2026
Seite 1–12
45. Jahrgang
1. Dezember 2026

Professor Dr. Mario Martini und Wiss. Mitarbeiter Cirus Petzold*

Öffentlich und doch geheim: homomorph verschlüsselte Stimmabgabe als Wegbereiter für Online-Wahlen

Am Beispiel von Personalratswahlen

Von überall per Mausklick statt mit Stift im Wahllokal zu wählen, klingt verlockend. Doch digitale Wahlformate gelten bisher als kaum überprüfbar, fehleranfällig und manipulierbar. Dieser Skepsis entzieht die technische Entwicklung zunehmend die Grundlage. Denn die Blockchain-Technologie und die homomorphe Verschlüsselung heben die Integrität des Wahl- und Auszählungsprozesses auf eine neue Stufe. Am Beispiel der bayerischen Personalratswahlen zeigt der Beitrag Wege auf, wie sich Online-Wahlen pro futuro mithilfe dieser Technologien in spezifischen Kontexten überprüfbar und sicher durchführen lassen.

I. Stift, Zettel, Urne und die „Flucht der Wähler" in der modernen Demokratie

Verwaiste Wahllokale, wartende Wahlhelfer und halb volle Urnen gehören immer häufiger zum Erscheinungsbild deutscher Wahlen. *Bundes- und Landtagswahlen* locken die Bürger zwar noch in vergleichsweise reicher Zahl an die Wahlurnen.[1] Doch bei *Kommunalwahlen* übt mancherorts nicht einmal jeder Zweite sein vornehmstes Bürgerrecht aus.[2] An Hochschulwahlen nimmt weniger als jeder siebte Wahlberechtigte teil.[3] Es zeichnet sich eine klare Tendenz ab: Je überschaubarer die Angelegenheit, desto stärker sinkt die Wahlbeteiligung.

Das Vakuum, das die niedrige Wahlbeteiligung hinterlässt, ist nicht unbedingt Ausdruck politischen Desinteresses. Vielmehr verlagert sich der politische Diskurs zunehmend in digitale Arenen: Internetforen sind zum Ort pluralistischen Meinungsaustauschs geworden; digitale Bürgeranhörungen und -befragungen[4] sowie Online-Petitionen erfreuen sich wachsender Beliebtheit.[5] Ihre Partizipationskanäle bestechen durch einen einfachen strukturellen Vorteil: Sie eröffnen einen niedrigschwelligen Zugang. Ob von der Terrasse aus oder unterwegs zwischen Tür und Angel: Es reichen wenige Klicks, um die eigene politische Position kundzutun.[6] Schwerfällige traditionelle Partizipationsformate geraten da schnell ins Hintertreffen.[7]

Auf den Wandel der Kommunikationswege reagiert das Wahlrecht bisher nur zögerlich. Erste Liberalisierungsschrit-

* Der Autor Martini ist Inhaber des Lehrstuhls für „Recht und Digitalisierung" an der UniBw München und Leiter des Themenbereichs „Digitale Transformation im Rechtsstaat" am Deutschen Forschungsinstitut für öffentliche Verwaltung. Der Autor Petzold ist Wissenschaftlicher Mitarbeiter am Lehrstuhl. Der Aufsatz geht auf das Drittmittelprojekt „Urban verifiziert" zurück, welches das Bundesministerium für Forschung, Technologie und Raumfahrt (BMFTR) im Rahmen der Förderrichtlinie „DATIpilot – Fördern & Lernen für Innovation und Transfer" gefördert hat. Soweit nicht anders vermerkt, erfolgte der letzte Abruf der Internetquellen am 12.8.2026.

1 Vgl. Die Bundeswahlleiterin, Wahl-Lexikon, https://www.bundeswahlleiterin.de/service/glossar/w/wahlbeteiligung.html; Brandt, Wie hoch ist die Wahlbeteiligung bei Landtagswahlen, https://de.statista.com/infografik/19187/wahlbeteiligung-bei-landtagswahlen/.

2 So etwa in Teilen bei den Kommunalwahlen in NRW im Jahr 2025, Die Landeswahlleiterin des Landes Nordrhein-Westfalen, Rangfolge Wahlbeteiligung – Kommunalwahlen 2025 in NRW, https://www.wahlergebnisse.nrw/kommunalwahlen/2025/aktuell/wahlbeteiligung.shtml.

3 Lenz/Hering, Uni-Demokratie: Studierende wählen kaum, https://correctiv.org/aktuelles/bildung/2020/08/09/uni-demokratie-studierende-waehlen-kaum/.

4 S. die Regelung des § 28 III KVG LSA, die auf den Vorschlag des Verfassers in seiner Stellungnahme für den Innenausschuss des Landtages zurückgeht: „Die Vertretung kann beschließen, zu Angelegenheiten des eigenen Wirkungskreises der Kommune eine Befragung der Bürger durchzuführen. […] Die Abstimmung kann auch als Onlineabstimmung erfolgen, soweit hinreichend sichere Vorkehrungen gegen Missbrauch und zur Sicherung der Integrität der Ergebnisermittlung getroffen werden." Martini, Stellungnahme für den Ausschuss für Inneres und Sport des Landtages Sachsen-Anhalt zu den §§ 25–28 KVG LSA-E (bürgerschaftliche Teilhabe), Textdokumentation der 38. Sitzung, Niederschrift 6/INN/38, S. 21.

5 Voss, Engagiert, Politisch, Digital?, 2021, S. 13 f.; Hill/Schliesky/Martini, Die Neubestimmung der Privatheit, 2014, 193 (195).

6 Cammerzell, Partizipation in einer digitalen Epoche, https://regierungsforschung.de/wp-content/uploads/2022/10/20102022_regierungsforschung.de_Cammerzell_digitale-Epoche-Partizipation.pdf, S. 3.

7 Strippel/Jokerst/Heger/Emmer, Politische Partizipation in Deutschland, 2024, S. 4.

te – etwa der Ausbau der Briefwahl – haben am *modus operandi* der Stimmabgabe mit Stift, Wahlzettel und Urne nichts Grundlegendes geändert. Die digitale Lebenswirklichkeit der Menschen scheint sich vom Status quo demokratischer Wahlen in Deutschland zunehmend zu entkoppeln.

II. Der Grundsatz der Öffentlichkeit der Wahl

Dem Wunsch, per Klick statt Kreuz zu wählen, schiebt das Grundgesetz nicht ausdrücklich einen Riegel vor. Dass Wahlen dennoch bisher das Mantra „Paper by Default" beschwören, hat gleichwohl einen verfassungsrechtlichen Grund: den ungeschriebenen Grundsatz der Öffentlichkeit von Wahlen. Das BVerfG leitet ihn aus den Vorgaben des Art. 38 I 1 GG in Verbindung mit den verfassungsrechtlichen Grundentscheidungen für Demokratie, Republik und Rechtsstaatlichkeit (Art. 20 I, II GG) ab:[8] „[A]lle wesentlichen Schritte der Wahl [unterliegen] öffentlicher Überprüfbarkeit"[9] – vor allem die Wahlhandlung und die Ermittlung des Wahlergebnisses. Denn nur wenn hinreichende öffentliche Kontrolle besteht, kann der Einzelne darauf zählen, dass das System seine Stimme unverfälscht erfasst und in das Wahlergebnis einbezieht. Auf diesem Fundament baut das Vertrauen in den Urakt der Demokratie auf.[10]

Die öffentliche Kontrolle der Wahl sichert auch die anderen Wahlrechtsgrundsätze des Art. 38 I 1 GG als Flankenschutz ab: Sie verbürgt, dass jeder Berechtigte Zugang zur Wahl hat (Allgemeinheit), jeder Stimme die gleiche Bedeutung zukommt (Gleichheit) und zwischen Wähler sowie Gewähltem kein Dritter tritt, der das Wahlergebnis beeinflusst (Unmittelbarkeit).[11] Ist die Öffentlichkeit der Wahl nicht gewährleistet, gefährdet dies daher auch die anderen Wahlrechtsgrundsätze.

Die traditionelle Papierwahl genügt den Anforderungen des Öffentlichkeitsgrundsatzes mühelos: Sowohl der Wähler selbst als auch außenstehende Dritte können dank ihres Zutrittsrechts (§ 31 BWahlG, § 54 BWahlO) die wesentlichen Schritte des Wahlvorgangs beobachten und nachvollziehen.[12] Das reicht von der Identifikation des Wählers im Wahllokal über die Ausgabe des Wahlzettels, den Weg in die Wahlkabine, das Einwerfen in die Urne bis hin zu deren Öffnung und Auszählung.

Dass digitale Wahlinstrumente dem Öffentlichkeitsgrundsatz genügen, versteht sich dagegen nicht von selbst: Sie lassen sich tiefgreifender und weitreichender manipulieren und sind auch spürbar fehleranfälliger. Wer keine informationstechnischen Spezialkenntnisse besitzt, vermag solche Eingriffe und Störungen bei digitalen Wahlen nicht zu erkennen. Die Öffentlichkeit kann ihre Kontrollfunktion bei Digitalwahlen daher nur ungleich schwerer erfüllen.[13]

1. Inhaltliche Anforderungen

So sehr der Grundsatz der Öffentlichkeit Einsehbarkeit voraussetzt, so wenig verlangt er, dass alle Bürger jeden einzelnen Schritt im Wahlverfahren bis ins Detail kontrollieren oder nachvollziehen können. Das illustriert schon der Umstand, dass die Stimmabgabe geheim bleiben muss (vgl. Art. 38 I 1 GG).[14] Erforderlich, aber auch ausreichend ist, dass sich der prozedurale Lauf aller wesentlichen Schritte des Wahlverfahrens zuverlässig „ohne besondere technische Vorkenntnisse" nachvollziehen lässt.[15]

Anzeigen, die nur bestätigen, dass ein System die abgegebene Stimme registriert hat, reichen dafür jedenfalls nicht aus. Sie machen Fehler und Manipulationen nicht hinreichend überprüfbar. Ebenso wenig genügt es, wenn die Anzeige lediglich den Rechenprozess wiedergibt. Denn das belegt nur, *dass* überhaupt ein Verarbeitungsprozess stattfand, macht aber Manipulationen oder Verarbeitungsfehler selbst nicht sichtbar.[16] Der Öffentlichkeitsgrundsatz erfordert vielmehr, auch die *Richtigkeit* der Verarbeitung kontrollieren zu können. Technische und organisatorische Prüfungen vor dem Wahlakt bieten daher ebenso wenig ausreichende Gewähr für die Öffentlichkeit der Wahl. Kontrollen der Geräte verheißen zwar Manipulations- und Fehlerfreiheit zum Zeitpunkt der Untersuchung. Sie ermöglichen aber weder vertiefte Einblicke in das Innenleben des eingesetzten Wahlgeräts noch verhindern sie nachträgliche Manipulationen oder Fehler.[17]

Ausreichen kann es jedoch, die Stimmen ergänzend zur elektronischen Aufnahme auch „anderweitig", also in tradierter Papierform, zu erfassen, so dass das System die Stimme nicht ausschließlich auf einem elektronischen Speichermedium, sondern auch in einer greifbaren Form ablegt.[18] Dafür gibt es zwei Möglichkeiten: Entweder kontrolliert ein Papierprotokoll die elektronisch abgegebenen Stimmen oder das System erfasst die schriftlich abgegebenen Stimmen zusätzlich elektronisch.[19]

Die Papierdurchschrift ist aber weder zwingend erforderlich noch schließt die Öffentlichkeitskontrolle Speicherformate aus, die ausschließlich digital operieren.[20] Das BVerfG lässt zumindest bewusst offen, ob auch andere technische Wege dem Wähler ein nachvollziehbar begründetes Vertrauen in die ordnungsgemäße Stimmermittlung vermitteln und damit den inhaltlichen Anforderungen des Öffentlichkeitsgrundsatzes genügen.[21]

2. Anwendbarkeit auf Personalratswahlen

Den Grundsatz der Öffentlichkeit leitete das BVerfG unmittelbar nur für die Bundestagswahlen aus dem GG ab. Ob und inwieweit er als verfassungsrechtlicher Eckpfeiler eins zu eins auch Maßstäbe für andere Wahlen setzt, ist weniger klar.[22]

Für die *Sozialversicherungswahlen* hat der Bundesgesetzgeber den Öffentlichkeitsgrundsatz in § 45 II 1 SGB IV explizit einfachgesetzlich verankert: „Die Wahlen sind frei, geheim und öffentlich". Daraus leitet er jedoch keine unüberwindbare Hürde für Online-Wahlen ab. Ab 2020 steckten die §§ 194a ff. SGB V aF zeitlich begrenzt die rechtlichen Rahmenbedingungen für das „Modellprojekt zur Durchführung von Online-Wahlen bei den Krankenkassen" im Jahr 2023 ab. Jeder Wahlberechtigte erhielt (per Brief) ein individuelles Wahlkennzeichen, das im Zusammenspiel mit weiteren Identifikatoren den Zugang zur digitalen Wahlplattform eröffnete. Diese war über alle gängigen Internetbrowser zugänglich – also über PC, Tablet oder Smartphone erreichbar. Mit wenigen Klicks konnte jeder Wahlberechtig-

8 BVerfGE 123, 39 (68) = NVwZ 2009, 708 (709).
9 BVerfGE 123, 39 (70) = NVwZ 2009, 708 (710).
10 BVerfGE 123, 39 (68, 70) = NVwZ 2009, 708 (709 f.).
11 BeckOK GG/Butzer, 65. Ed. 2026, GG Art. 38 Rn. 145.
12 Will NVwZ 2009, 700 (702 f.). Ähnl. Schiedermair JZ 2009, 572 (574).
13 BVerfGE 123, 39 (72) = NVwZ 2009, 708 (710 f.).
14 So bereits BVerfGE 121, 266 (291) = NVwZ 2008, 991 (992).
15 BVerfGE 123, 39 (69 f.) = NVwZ 2009, 708 (710).
16 BVerfGE 123, 39 (72 f.) = NVwZ 2009, 708 (711).
17 BVerfGE 123, 39 (74 f.) = NVwZ 2009, 708 (711).
18 BVerfGE 123, 39 (73) = NVwZ 2009, 708 (711).
19 BVerfGE 123, 39 (73 f.) = NVwZ 2009, 708 (711).
20 Hill/Schliesky/Martini, Die Neubestimmung der Privatheit, 2014, 193 (196). AA wohl Omlor JZ 2022, 649 (654).
21 BVerfGE 123, 39 (74) = NVwZ 2009, 708 (711).
22 Bretthauer/Spiecker gen. Döhmann NZS 2020, 241 (243); Buchmann/Roßnagel K&R 2009, 543 (546).

te seine Stimme abgeben und deren weiteres Schicksal im Anschluss mithilfe einer zusätzlichen App auch überprüfen.[23]

Wie erfolgreich das Projekt war, beurteilen Beobachter zwar unterschiedlich.[24] Öffentlichkeitsgrundsatz und Online-Wahlen vereinen sich seitdem aber zumindest rechtlich zu einem harmonischen Miteinander. Die Vorgaben gelten nun für alle Zweige der Sozialversicherung, in denen Sozialversicherungswahlen stattfinden (s. insbesondere § 54 I 2 SGB IV, der neben der brieflichen die elektronische Stimmabgabe erlaubt, „wenn die Satzung des Versicherungsträgers die Möglichkeit der Online-Wahl ergänzend vorsieht").[25]

Ausdrücklich erlaubt ist die elektronische Wahl auch für die Wahl der stimmberechtigten Mitglieder der *Satzungsversammlung von Rechtsanwaltskammern* (§ 191b II 2 BRAO). Bayern lässt für *Hochschulwahlen* ebenfalls die Option zu, diese auf der Grundlage einer Satzung ganz oder teilweise elektronisch durchzuführen (Art. 48 II 2 BayHIG). Das Land Sachsen-Anhalt gestattet Online-Abstimmungen auf kommunaler Ebene: (Nicht bindende) *Befragungen der Bürger* zu Angelegenheiten des eigenen Wirkungskreises der Kommune sind grundsätzlich auch online möglich (§ 28 III 4 KVG LSA).[26]

Bei *Betriebsratswahlen* haben die Arbeitsgerichte Online-Wahlen bisher kassiert, auch wenn das einschlägige Wahlrecht (insbesondere die Wahlordnung des BetrVG) den Öffentlichkeitsgrundsatz nicht ausdrücklich aufstellt.[27] Die Regierungskoalition aus CDU/CSU und SPD strebt aber nunmehr an, Online-Wahlen als Option im BetrVG ausdrücklich zu verankern.[28] Sie greift damit die Bemühungen der vergangenen Legislaturperiode wieder auf, eine Rechtsgrundlage für Digitalwahlen zu etablieren, die dem Öffentlichkeitsgrundsatz ausreichend Rechnung trägt.[29] Ursprünglich sollte bereits die Betriebsratswahl im März 2026 online stattfinden, sofern hinreichende technische Sicherheitsmaßstäbe bestehen (§ 18b BetrVG-E). Dazu ist es jedoch nicht gekommen. Da die nächsten Betriebsratswahlen erst im Jahr 2030 anstehen, ist der Plan aktuell wieder zum Erliegen gekommen.

Für *Personalratswahlen* begnügen sich sowohl der Bundes- als auch der bayerische Gesetzgeber bisher mit der Vorgabe „geheimer und unmittelbarer Wahl" (§ 19 I BPersVG; Art. 19 I BayPVG). Ein ausdrückliches Gebot der Öffentlichkeit kennen die Personalvertretungsgesetze ebenso wenig wie die untergesetzlichen Vorschriften zur Personalratswahl. Änderungen sind gegenwärtig – zumindest im Koalitionsvertrag – nicht vorgesehen, aber sehr erwägenswert. Denn Personalratswahlen sind auf den ersten Blick als Experimentierfeld für Online-Wahlen prädestiniert: Sie vollziehen sich im abgegrenzten Rahmen der jeweiligen Dienststelle, so dass sich negative Auswirkungen gescheiterter Digitalisierungsversuche in Grenzen halten. Erfolge können hingegen auch für andere politische Ebenen wertvolle Erkenntnisse liefern und so eine langfristige Ausstrahlungswirkung entfalten. Häufig verfügen Beschäftigte im öffentlichen Dienst überdies auch dank ihres Dienstausweises bereits in hinreichendem Maße über digitale Identitäten, die für eine Online-Wahl erforderlich sind. Umgekehrt ist das Bedürfnis, durch Online-Wahlen sinkenden Wählerzahlen entgegenzuwirken, bei Personalratswahlen aber weniger stark ausgeprägt. Denn bislang bleibt die Personalratswahl von dem Negativtrend niedriger Wahlbeteiligung weitestgehend verschont.[30] Als gewählte Interessenvertretung der Beschäftigten im öffentlichen Dienst ist der Personalrat das zentrale Sprachrohr und der Repräsentant der Belegschaft. Seine Arbeit erfreut sich großer Beliebtheit.[31] Diesen Rückhalt im Verwaltungsalltag und die Autorität des Amtes droht der Personalrat zu verlieren, wenn seine Legitimität nicht auf rechtlich sicherem Fundament steht.

Die Grundsätze der Bundestagswahl unbesehen auf die Personalratswahl zu übertragen, versteht sich gleichwohl nicht von selbst. Denn die demokratische Legitimationskette des Personalrats ist anders geknüpft als diejenige des Bundestages: Dessen Zusammensetzung baut auf den Erst- und Zweitstimmen aller Wahlberechtigten auf; die gewählten Abgeordneten sind Vertreter des ganzen Volkes (Art. 38 I 2 GG).[32] Bei der Personalratswahl spalten die Personalvertretungsgesetze die Wählerschaft hingegen in mehrere Gruppen auf: Art. 5 BayPVG unterscheidet (wie auch § 5 S. 1 BPersVG) zwischen Beamten und Arbeitnehmern. Beide Gruppen wählen in getrennten Wahlgängen ihre eigenen Gruppenvertreter (Art. 19 II 1 BayPVG; § 19 II 1 BPersVG). Im Kollegialorgan Personalrat sind sie entsprechend ihrer Stärke in der Belegschaft vertreten (Art. 17 I 1 BayPVG; § 17 I 1 BPersVG).

Personalrat und Bundestag unterscheiden sich auch funktionell grundlegend.[33] Der Bundestag überführt als Legislativorgan politische Entscheidungen in abstrakt-generelle Gesetze, die für alle Bürger gelten. Der Personalrat ist hingegen vorrangig mit überwachenden und administrativen Aufgaben betraut (Art. 69 BayPVG; § 69 BPersVG). Dienstvereinbarungen (Art. 73 BayPVG; § 63 BPersVG) kommt zwar normative Wirkung zu.[34] Sie betreffen aber einen überschaubaren Kreis interner Angelegenheiten und gelten nur für Beschäftigte der jeweiligen Dienststelle.[35] Der Wirkkreis des Personalrates beschränkt sich also *qua natura* auf den Mikrokosmos der jeweiligen Dienststelle. Normative Befugnisse für die breite Masse kommen ihm nicht zu. Weder legitimiert ihn die breite Öffentlichkeit unmittelbar noch berührt seine Tätigkeit Außenstehende.

Dass Bundestag und Personalrat sich in Wahl, Zusammensetzung und Aufgaben grundlegend unterscheiden, impliziert aber nicht notwendig, den Wahlrechtsgrundsatz der Öffentlichkeit bei der Personalratswahl zu überspielen. Obgleich Bundes- und Landesgesetzgeber den Personalrat in mehrere Gruppen aufgliedern, soll er die kollektiven Interessen aller beschäftigten Personen vertreten und damit alle Gruppen repräsentieren.[36] Die Stellung als Mitglied der Personalvertretung entspricht einem Mandat, das grundsätzlich nicht

23 Bräuning/Schippers/Rehfeld/Stautz DuD 2024, 460 (461 f.).
24 Positiv etwa: Bundeswahlbeauftragter für die Sozialversicherungswahlen, Schlussbericht zu den Sozialwahlen 2023, S. 87; kritisch hingegen Becker/Kingreen, 9. Aufl. 2024, SGB V § 194d Rn. 3.
25 BR-Drs. 424/25, 55.
26 S. dazu den Vorschlag von Martini, Stellungnahme zu den §§ 25–28 LSA KVG-E (bürgerschaftliche Teilhabe) vom 13.10.2013, Textdokumentation der 38. Sitzung, Niederschrift 6/INN/38, S. 21.
27 LAG Hamburg 15.2.2018 – 8 TaBV 5/17, BeckRS 2018, 20356 Rn. 17.
28 Koalitionsvertrag zwischen CDU, CSU und SPD für die 21. Legislaturperiode, Verantwortung für Deutschland, S. 19.
29 BR-Drs. 588/24, 50.
30 Schmidt/Müller, Personalräte, 2025, S. 96.
31 Niehoff/Holst WSI Mitteilungen, 2022, 437 (441) zur Arbeit von Betriebs- und Personalräten während der Corona-Pandemie.
32 Dürig/Herzog/Scholz/Grzeszick, 109. EL 2026, GG Art. 20 Rn. 69.
33 Ähnl. in Bezug auf die Sozialwahlen Bretthauer/Spiecker gen. Döhmann NZS 2020, 241 (244).
34 Zur Rechtsnatur der Dienstvereinbarung Richardi/Dörner/Weber/Annuß/Annuß, 6. Aufl. 2024, BPersVG § 63 Rn. 11 mwN.
35 BeckOK BPersVG/Ricken, 23. Ed. 2026, BPersVG § 63 Rn. 2 ff., 22 ff.
36 Vgl. BVerfGE 28, 314 (322) = BeckRS 1970, 106848; BVerfGE 51, 77 (86 f.) = NJW 1979, 1875 (1875).

entziehbar ist.[37] Vor diesem Hintergrund spiegelt der Personalrat das repräsentativ-demokratische Modell des Bundestages „im Kleinen“ für den Bereich der Dienststelle wider.[38] Für seine Wahl müssen daher im Grundsatz auch die gleichen demokratischen Wahlrechtsgrundsätze gelten.[39] Das gilt auch für die Öffentlichkeit der Wahl. Denn nur das Vertrauen der Wähler in den ordnungsgemäßen Wahlverlauf stützt die Verbindlichkeit des Wahlergebnisses.

3. Entscheidungsspielraum des Gesetzgebers

Der Grundsatz der Öffentlichkeit der Wahl gilt nicht absolut. Kollidierende verfassungsrechtliche Schutzgüter, insbesondere die Wahlrechtsgrundsätze des Art. 38 I 1 GG, gestatten Ausnahmen von dem Gebot öffentlicher Kontrolle, solange sein Kerninhalt gewahrt bleibt.[40] Keines der Verfassungsprinzipien genießt dabei prinzipiellen Vorrang gegenüber den anderen. Sie sind vielmehr behutsam gegeneinander auszugleichen.[41] Diese Aufgabe obliegt grundsätzlich dem Gesetzgeber.[42] Die Verfassung räumt ihm einen weiten Spielraum ein, wie er das Wahlverfahren ausgestaltet (Art. 38 III GG). Dies schließt auch die technischen Aspekte des Wahlvorgangs – einschließlich des Einsatzes technischer Geräte – ein.[43] Innerhalb der verfassungsrechtlichen Grenzen, welche die Wahlrechtsgrundsätze ziehen,[44] ist es daher unerheblich, ob die einfachgesetzliche Ausgestaltung der Wahl zweckmäßig oder rechtspolitisch wünschenswert ist.[45] Sofern der Gesetzgeber die Anforderungen des Öffentlichkeitsgrundsatzes nicht verletzt, ist er nicht daran gehindert, den Modus der Wahlhandlung neu zu gestalten.[46]

Digitale Wahlformate, die die Stimmabgabe von Wahllokalen oder Briefen entkoppeln, fördern zwar grundsätzlich die Allgemeinheit der Wahl.[47] Eine höhere Wahlbeteiligung heilt aber nicht die Mängel, die eine manipulationsbedingt ungültige Wahl nach sich zieht. Nicht zuletzt zeigen Online-Wahlformate in praxi bisher uneinheitliche Auswirkungen auf die Wahlbeteiligung.[48] „Remote“-Wahlformate stechen daher nicht per se als Trumpf jeden Einwand.[49] Die nachvollziehbare Intention, durch eine elektronische Stimmabgabe die Wahlbeteiligung zu steigern, rechtfertigt daher nicht ohne Weiteres Abstriche beim Öffentlichkeitsgrundsatz.[50]

Auch das Ziel, durch den Einsatz von Wahlcomputern ungewollt ungültige Stimmabgaben zu vermeiden, ist zwar legitim. Es rechtfertigt in den Augen des BVerfG aber noch nicht die damit verbundenen Einschränkungen der öffentlichen Kontrolle. Es schlägt stattdessen vor, analoge und digitale Stimmträger parallel einzusetzen, da auch dies ungültige Stimmen vermeiden kann – allerdings ohne den Öffentlichkeitsgrundsatz zu beschneiden.[51]

4. Zwischenfazit

Der ungeschriebene Wahlrechtsgrundsatz der Öffentlichkeit ist das verfassungsrechtliche Nadelöhr einer Digitalisierung von Wahlen. Er verlangt nicht weniger, als dass alle wesentlichen Schritte der Wahl öffentlich überprüfbar sind. Lässt sich nachvollziehen, dass jede einzelne Stimme unverfälscht erfasst wurde und Eingang in das Wahlergebnis gefunden hat, ist dem hinreichend Rechnung getragen. Erst wenn sich das öffentlich kontrollieren lässt, entsteht auch das Vertrauen in den ordnungsgemäßen Ablauf der Wahl, welches der Grundsatz der Öffentlichkeit verfassungsrechtlich absichern soll.

Das BVerfG erteilt elektronischen Wahlgeräten zwar keine generelle Absage. Wegen ihrer hohen Manipulations- und Fehleranfälligkeit sind sie allerdings verfassungsrechtlich heikel. Denn von außen lässt sich nur schwer nachvollziehen, ob die technischen Instrumente fehlerfrei arbeiten. Sie bleiben eine Blackbox.[52] Der konkrete Werdegang der Stimme von der Wahlkabine bis zur Auszählung liegt im Dunkeln. Geboten ist nicht allein, dass die Geräte die Stimme als solche richtig erfassen. Diese muss auch korrekt in das Wahlergebnis einfließen. Sicherstellen lässt sich das vor allem (aber nicht nur) mit hybriden Verfahren, bei denen sich elektronische und schriftliche Stimmabgabe gegenseitig kontrollieren.

Der Öffentlichkeitsgrundsatz gilt nicht nur für Bundestagswahlen. Seine Anforderungen strahlen auch bis auf die Ebene der Personalratswahlen aus. Alle technischen Möglichkeiten, um digitale Wahlen durchzuführen, müssen im Ergebnis „ein auf Nachvollziehbarkeit gegründetes Vertrauen des Wahlvolks in die Korrektheit des Verfahrens bei der Ermittlung des Wahlergebnisses ermöglichen“.[53]

III. Blockchain und homomorphe Verschlüsselung als Gamechanger?

Einen technischen Lösungsansatz, um Vorbehalten fehlender Nachvollziehbarkeit und Manipulationsanfälligkeit entgegenzutreten, zeigen kryptographische Verfahren auf. Sie verschlüsseln Informationen und wahren so deren Vertraulichkeit, Integrität, Authentizität sowie Verbindlichkeit.

Die Distributed-Ledger-Technologie bedient sich kryptographischer Verfahren, um Transaktionen sicher und zugleich von außen nachvollziehbar abzuwickeln. Bei der validierten Erfassung und Auszählung ausgeübter Rechte kann die kryptographische Absicherung ihre Stärken besonders ausspielen. Sie birgt dadurch das Potenzial, Wahlen so ins digitale Zeitalter zu überführen, dass die technische Ausgestaltung dem Gebot der Öffentlichkeit der Wahl entspricht.

Dafür muss die Technik aber allen Anforderungen an die Nachvollziehbarkeit und Überprüfbarkeit standhalten (1.), ohne Fehler und Manipulationen zu begünstigen (2.). Auch der einzelne – nicht technisch versierte – Bürger muss dies kontrollieren können (3.). Sie muss zudem solchen Risiken hinreichend sicher entgegenwirken, die außerhalb des Einflussbereichs der Wahlbehörde liegen (4.). Nur dann legt die kryptographische Verschlüsselung ein solides Fundament des Vertrauens, das demjenigen in die Papierwahl in nichts nachsteht.

37 MHdB ArbR/Germelmann, 6. Aufl. 2024, § 360 Rn. 59.
38 OVG Weimar 20.3.2001 – 5 PO 407/00, BeckRS 2001, 30473709.
39 Vgl. BVerfGE 71, 81 (93 ff.) = NJW 1986, 1093; Bremke LKV 2004, 102 (106 f.); Richardi/Dörner/Weber/Annuß/Dörner, 6. Aufl. 2024, BPersVG § 19 Rn. 3; Klein/Stuttmann PersVertretungsR NRW, 2. Aufl. 2024, S. 51 jedoch mit Beschränkungen in personeller Hinsicht; BeckOK BPersVG/Behmenburg, 23. Ed. 2026, BPersVG § 19 Rn. 1. Für einen weiteren Spielraum im Bereich der Betriebs- und Personalratswahlen: Buchmann/Roßnagel K&R 2009, 543 (546); ähnl. in Bezug auf die Sozialwahl Bretthauer/Spiecker gen. Döhmann NZS 2020, 241 (242 ff.) mwN.
40 BVerfGE 123, 39 (75) = NVwZ 2009, 708 (711).
41 BVerfGE 134, 25 (30) = NVwZ 2013, 1272 Rn. 15.
42 BVerfGE 123, 39 (70 f.) = NVwZ 2009, 708 (710).
43 BVerfGE 123, 39 (71) = NVwZ 2009, 708 (709).
44 BVerfGE 123, 39 (71) = NVwZ 2009, 708 (710).
45 BVerfGE 123, 39 (71) = NVwZ 2009, 708 (710).
46 Schiedermair JZ 2009, 572 (573).
47 Ehrenberg-Silies/Busch-Heizmann/Lüddecke, E-Voting – alternative Wahlformen und ihre Absicherung, S. 23 ff.
48 Ehrenberg-Silies/Busch-Heizmann/Lüddecke, E-Voting – alternative Wahlformen und ihre Absicherung, S. 23 ff.
49 AA Bretthauer/Spiecker gen. Döhmann NZS 2020, 241 (245).
50 BVerfGE 123, 39 (75) = NVwZ 2009, 708 (711).
51 BVerfGE 123, 39 (75 f.) = NVwZ 2009, 708 (712).
52 Schiedermair JZ 2009, 572 (574).
53 BVerfGE 123, 39 (74) = NVwZ 2009, 708 (711).

1. Überprüfbarkeit des Wahlverfahrens

Auf den ersten Blick läuft die kryptographische Verschlüsselung den Anforderungen an die öffentliche Überprüfbarkeit des Wahlverfahrens diametral entgegen. Denn sobald eine Information verschlüsselt ist, kann die Öffentlichkeit sie nicht unmittelbar prüfen.

Wahlen überprüfbar zu machen, wie es der Öffentlichkeitsgrundsatz gebietet, verlangt aber nicht, in den *Inhalt* der abgegebenen Stimme Einsicht nehmen zu können. Es genügt, den *prozeduralen Ablauf* der Wahlen in einer Weise nachvollziehbar zu machen, dass sowohl die Wähler selbst als auch beobachtende Dritte kontrollieren können, ob das System die einzelne Stimme unverfälscht erfasst und in das Wahlergebnis übernimmt.

Bettet man die kryptographische Verschlüsselung in eine Blockchain[54] ein, greifen beide Technologien wie Bauteile eines Gefüges ineinander: Die Blockchain-Infrastruktur stellt sicher, dass die Kette von der einzelnen Stimme bis zum gesamten Wahlergebnis nachvollziehbar bleibt (a).[55] Die kryptographische Verschlüsselung hält die Stimmabgabe geheim (b).[56]

a) Transparenz durch Blockchain

Transparenz gehört zur „DNA“ der Blockchain-Technologie. Ihr Code beruht auf dem Grundprinzip, jedem Teilnehmer Einsicht in die Handlungen der anderen zu gewähren. Auf diese Weise schließt sie Vertrauenslücken zwischen Personen, die einander nicht kennen. Jeder einzelne Block speichert neben der Information über die abgegebene Stimme auch einen eigenen, einmaligen „Hash“. Dieser macht die Information des einzelnen Blocks eindeutig identifizierbar.[57] Jeder neue Block führt nicht nur seinen eigenen Hash mit. Er nimmt zugleich den vorausgehenden Hash-Wert in den Informationsstrang mit auf. Dadurch bildet er den Weg der jeweiligen Stimme lückenlos ab.[58] So entsteht eine in sich geschlossene Kette: Jeder Block ist zum einen für sich gesichert, zum anderen schließt er alle vorausgehenden Glieder der Kette ein. Ein neuer Block lässt sich der Kette aus bereits bestehenden Stimmblöcken nur dann anhängen, wenn er den Anforderungen des Konsensmechanismus genügt,[59] den sog. Validatoren prüfen.[60] Die dezentral bei allen Validatoren gespiegelten Kopien stellen zugleich sicher, dass niemand die Kette nachträglich ändert – andernfalls decken sich die Kopien nicht mehr. Diese lückenlose Verkettung sichert nicht nur die Stimmen. Sie macht zugleich den gesamten Wahlvorgang überprüfbar. Fällt ein einzelnes Glied weg, reißt die Kette. Falschzählungen treten dadurch nicht erst am Ende des Wahlgangs zutage, sondern in Echtzeit – sobald sie geschehen, weil die Beteiligten die Kette dauerhaft miteinander abgleichen.[61]

Diesen technischen Vorgang können nicht nur diejenigen kontrollieren, die aktiv an der Stimmen-Kette mitwirken (*individuelle Verifizierbarkeit*). Auch Unbeteiligten steht bei einer öffentlich einsehbaren Blockchain das digitale Wahllokal offen (*universelle Verifizierbarkeit*).[62] So kann auch der Nichtwähler oder gar ein nicht wahlberechtigter Dritter den Werdegang der Blockchain beobachten.[63] Parallel dazu kann der Wähler durchgängig kontrollieren, ob die Blockchain seine Stimme ordnungsgemäß verbucht.[64] Auch nach Abgabe der Stimme kann er nachvollziehen, ob das System seine individuelle Transaktion korrekt registriert und eingebunden hat.[65] Verlorengegangenen oder nicht mitgezählten Stimmen tritt die Blockchain so bereits auf erster Ebene entgegen[66] und schließt sie faktisch aus.[67]

b) Geheimheit durch Kryptographie

Je besser ein Wahlvorgang überprüfbar ist, umso stärker droht dies die Geheimheit der Wahl einzuschränken: Lässt sich jede Stimme über den gesamten Wahlverlauf hinweg beobachten, eröffnet sich damit im Grundsatz auch Dritten der Blick auf die individuelle Stimmabgabe.[68] Denn jeder Block, der auf den Informationen der vorausgehenden Kette aufbaut, birgt die Gefahr, die Stimme des einzelnen Wählers offenzulegen. Um dem entgegenzuwirken, arbeitet die Kryptographie an Protokollen, die den Inhalt der abgegebenen Stimme verbergen, sie aber gleichwohl hinreichend sicher auszählbar machen.

Eines dieser Verfahren ist die *blinde Signatur*. Ihr Funktionsprinzip lehnt sich an die Idee des analogen Briefumschlags aus durchpausendem Kohlepapier an. Der Wähler legt seinen ausgefüllten Stimmzettel in einen digitalen Briefumschlag, der mit digitaler Kohledurchschrift versehen ist, und identifiziert sich gegenüber der Wahlbehörde. Diese signiert den geschlossenen Briefumschlag blind und verbürgt damit seine Wahlberechtigung. Die Signatur drückt sich durch das digitale Kohlepapier auf den darin liegenden Stimmzettel durch, ohne dass die Wahlbehörde den Inhalt der Stimme kennt.[69] Ein separater Server leitet die Stimme mit der gültigen Unterschrift an die digitale Wahlurne weiter. Die Identität des Wählers und die Stimme bleiben so strikt voneinander getrennt. Niemand kann die Stimme nachträglich fälschen oder nachvollziehen, wer welche Stimme abgegeben hat.[70]

Das System krankt allerdings an einem entscheidenden Nachteil: Nur die am Wahlverfahren Beteiligten können blinde Signaturverfahren nachvollziehen. Eine universelle Verifizierbarkeit stellt das Verfahren nicht sicher.[71]

Die *homomorphe Verschlüsselung* verheißt, dieses wahlrechtliche Versprechen einzulösen. Sie eröffnet auch unbeteiligten Dritten die Möglichkeit, den ordnungsgemäßen Wahlablauf zu kontrollieren.[72] Ihr Verschlüsselungssystem verdeckt das digital gesetzte Kreuz und macht es gleichwohl

54 „Die eine Blockchain“ gibt es nicht. Es handelt sich vielmehr um ein Technologiekonzept mit vielen verschiedenen Ausgestaltungsformen.
55 Hackmann K&R 2019, 777 (779).
56 Vgl. BSI, Ende-zu-Ende Verifizierbare Onlinewahlen: Handlungsleitfaden für Wahlorganisatoren, S. 8 ff.
57 Meinel/Gayvoronskaya, Blockchain, 2020, S. 20.
58 Leupold/Wiebe/Glossner IT-R/Baur/Brügmann/Sedlmeier/Urbach, 4. Aufl. 2021, Kryptowährungen, Rn. 11.
59 Islam/Pal/Samanta ua/Mookherji/Vanga/Prasath, Blockchain Technology for Emerging Applications, 2022, 239 (251 f.).
60 SWK-Legal Tech-Steinrötter/Stamenov, 2023, Blockchain, Rn. 9.
61 Košt’ál/Bencel/Ries/Kotuliak IEEE, International Conference on Software Engineering and Service Sciences (ICSESS), 2019, 592 (595).
62 Vgl. Martini/Weinzierl NVwZ 2017, 1251 (1252).
63 Shuker/Hussain, Building Secure E-Voting Systems: A Blockchain Approach for Transparent Democracy, S. 2.
64 Berenjestanaki/Barzegar/El Ioini/Pahl Electronics 2024, 13:1, 17, S. 13; Mast JZ 2021, 237 (238). Kritisch zur Einsehbarkeit der eigenen Stimme wegen der Gefahr des Stimmenkaufs Xia/Tong/Xiao/Chang IET Information Security 2018, 247 (247 f.).
65 Mast JZ 2021, 237 (238).
66 BSI, Ende-zu-Ende Verifizierbare Onlinewahlen: Handlungsleitfaden für Wahlorganisatoren, S. 6.
67 BSI, Ende-zu-Ende Verifizierbare Onlinewahlen: Handlungsleitfaden für Wahlorganisatoren, S. 6.
68 Klenk/Nullmeier/Wewer/Bätge/Weiler, Handbuch Digitalisierung in Staat und Verwaltung, 2. Aufl. 2025, 335 (339).
69 Chaum CRYPTO 1982, 199 (200).
70 Ding/Chakrabarti/Chakraborty ua/Jhunjhunwala/Das/Paul, Proceedings of the Second International Conference on Advanced Computing and Systems, 2026, 314 (326).
71 Qu/Wu/Zang/Liu/Wang Concurrency and Computation: Practice and Experience 2022, 34:16, e5817, S. 3.
72 BSI, Technische Richtlinie TR-03169, Version 1.1, S. 26.

auszählbar. Dadurch gelingt es ihr, elektronisch abgegebene Stimmen zu verifizieren und zu aggregieren, ohne individuelle Wahlentscheidungen preiszugeben.[73]

Wie bereits der aus dem Griechischen stammende Begriff „homomorph" („gleiche Form") andeuten soll, zeichnet sich das Verfahren durch Strukturtreue zwischen der Ausgangs- und Endinformation aus. Dahinter steckt eine im Grundsatz einfache technische Idee: Es verschlüsselt eine Stimme nach kryptographischen Regeln so, dass sich die Daten trotz Verschlüsselung weiterverarbeiten lassen.[74] Damit befreit die Technologie den Anwender aus einem Dilemma: Daten waren bisher entweder lesbar oder verschlüsselt. Die homomorphe Verschlüsselung macht beides gleichzeitig möglich: Sie ebnet einen Weg, Berechnungen auf verschlüsselten Daten durchzuführen und die Kontrolle über den gesamten Datenverarbeitungsprozess gleichwohl in den Händen des Dateninhabers zu belassen. Der verschlüsselte Datensatz behält also seine algebraischen Strukturen auch nach der Verschlüsselung. Das erlaubt es, mit den Daten zu rechnen, ohne den Inhalt vorher zu entschlüsseln.[75]

Bei einer homomorphen Verschlüsselung behält allein der Wähler die Hoheit über die Einsichtnahme in die Daten.[76] Nur er kann seine Stimme wieder entschlüsseln.[77] Sobald die verschlüsselten Stimmen in die digitale Wahlurne purzeln, kombiniert das System sie miteinander, ohne sie entschlüsseln zu müssen. So aggregieren sich die verschlüsselten Einzelstimmen zu einem ebenfalls verschlüsselten Wahlergebnis.[78] Die Wahlbehörde kann nur das Endergebnis der Stimmauszählung entschlüsseln und einsehen;[79] der Blick auf die einzelne Stimme bleibt ihr verwehrt.[80] So verschlüsselt, speichert und verarbeitet das System die Daten und ermittelt das Wahlergebnis, ohne je auf den Inhalt der Stimme zurückzugreifen.

Die Öffentlichkeit kann und darf das Wahlergebnis zwar nachvollziehen. Sie darf dafür aber die Stimmauszählung nicht bis auf die individuelle Stimme herunterbrechen. Gleichwohl muss die Allgemeinheit kontrollieren können, dass sich bei der Verarbeitung verschlüsselter Datensätze kein Rechenfehler eingeschlichen hat. Dafür eignet sich insbesondere das Konzept des *Zero-Knowledge-Proofs*.[81] Dieses Beweisverfahren legt weder die zugrundeliegenden *Daten* noch das errechnete *Gesamtergebnis* offen. Es belegt allein die Richtigkeit des *Rechenweges*, der beide miteinander verbindet.[82] Technisch gelingt dies, indem das Verfahren den Rechenprozess in mathematische Prüfregeln übersetzt, die sich nur mit vorgegebenen Parametern lösen lassen.[83] Daraus erwächst dann ein gültiger Nachweis, wenn das Verfahren jede einzelne Stimme nach den vorgegebenen Regeln berechnet hat.[84] Dritte können prüfen, ob das Wahlergebnis zutreffend zusammengesetzt ist. Denn sie können mit einem spezifischen Schlüssel auf die Parameter zugreifen, aus denen das Verfahren die mathematische Formel erzeugt hat. Auf diese Weise können sie nur die Richtigkeit der Stimmauszählung prüfen, nicht aber auf weitere Elemente rückschließen.[85]

Der Zero-Knowledge-Proof lässt sich konzeptionell auch auf alle anderen Schritte des Wahlverfahrens übertragen, die einerseits geheim, andererseits überprüfbar bleiben müssen – etwa, wenn das System die Wahlberechtigung prüfen muss, ohne die Identität des Wählers offenzulegen. In diesem Fall weist der Wähler bereits bei der Stimmabgabe nach, dass seine Stimme den vorgegebenen Wahlregeln entspricht, insbesondere dass er zur Wahl berechtigt ist.[86] Der Wähler und seine Stimme selbst bleiben geheim.[87] Er generiert mit seiner Stimme einen kryptographischen Nachweis, der an seine Identität geknüpft ist. Dieser belegt, dass das Verfahren die Stimme nach den vorgegebenen Parametern verschlüsselt hat und damit der mathematischen Relation der Verschlüsselungstechnik entspricht. Nur Stimmen der Wahlberechtigten erzeugen einen passenden Nachweis, den dieser Beweis erfasst. Mit Hilfe des spezifischen Proof-Schlüssels können auch Dritte kontrollieren, ob der Wähler die Wahlregeln einhält, ohne Rückschlüsse auf ihn oder den Inhalt seiner Stimme ziehen zu können.[88]

Die Anonymität des Wählers birgt allerdings die Gefahr, doppelte Stimmabgaben zu begünstigen. Um dies zu verhindern, lässt sich der Zero-Knowledge-Proof um einen zusätzlichen *Nullifier* ergänzen. Dieser Marker setzt sich aus einem wählerspezifischen Wert und dem jeweiligen Wahlkontext zusammen.[89] So entsteht ein digitaler Fingerabdruck, der bei jedem weiteren Wahlversuch eine unverkennbare Spur hinterlässt.[90] Ist der Fingerabdruck bereits registriert, versagt das System einer daran gekoppelten neuen Stimme die Registrierung.[91] Da der Wähler im Zero-Knowledge-Proof seine Identität nicht offenlegt, lässt sich diese auch nicht über den Nullifier zurückrechnen.[92]

Die Kombination aus homomorpher Verschlüsselung und Zero-Knowledge-Proof ermöglicht im Ergebnis, durch moderne technische Verfahren einander widerstreitende Interessen in Einklang zu bringen, die sich dann gegenseitig sogar bestärken:[93] Obgleich die Stimmen geheim sind, lassen sie sich verifizierbar zusammenzählen. Einem so ausgestalteten digitalen Wahlformat gelingt der Balanceakt damit in ähnlicher Weise wie der analogen Papierwahl, die die Geheimheit der Wahl durch Kabine, Wahlumschlag und Urne gewährleistet, aber die korrekte Auszählung jederzeit nachvollziehbar macht. Nicht umsonst gilt die homomorphe Verschlüsselung als „heiliger Gral" der Kryptographie. Systeme, die sie einsetzen, sind technisch sehr anspruchsvoll, aber keine bloße Zukunftsmusik mehr. Nicht ohne Grund gelten

73 Singh/Gupta/Tyagi ua/Patel/Tandel/Sanghvi, Advances in Computing and Data Sciences, 2019, 565 (566).
74 Saini/Sayal/Govardhan ua/Salavi/Math/Kulkarni, Innovations in Computer Science and Engineering, 2019, 295 (298).
75 Acar/Aksu/Uluagac/Conti ACM CSUR, 2019, 51:4, 79, S. 2.
76 Zum Begriff der Datenhoheit s. Martini/Kolain/Neumann/Rehorst/Wagner MMR-Beil. 2021, 1 (18 f.).
77 Bremke LKV 2004, 102 (104 f.); Suwandi/Nasution/Azmi IEEE, International Conference on Informatics and Computing (ICIC), 2016, 329 (329).
78 Anggriane/Nasution/Azmi IEEE, International Conference on Informatics and Computing (ICIC), 2016, 338 (340).
79 Chaira/Cherroun/Aouag IJCA 2025, 819 (823).
80 Chaira/Cherroun/Aouag IJCA 2025, 819 (827).
81 BSI, Technische Richtlinie TR-03169, Version 1.1, S. 26. Zu weiteren Methoden s. etwa Bontekoe/Karastoyanova/Turkmen International Journal of Information Security, 2025, 24:3, 141, S. 1.
82 Lavin/Liu/Mohanty/Norman/Zaarour/Krishnamachari, A Survey on the Applications of Zero-Knowledge Proofs, v2, S. 2.
83 Vgl. Wätjen, Kryptographie, 3. Aufl. 2018, S. 216.
84 Vgl. Qureshi/Doshi/More/Joshi/Kumar JCTA 2025, 274 (278).
85 Miao IEEE, Proceedings of the 2023 International Conference on Software Engineering and Machine Learning, 2023, 346 (348 f.).
86 Park/Choi/Kim/Oh Cryptology ePrint Archive 2024, 1003, S. 8.
87 Zhou/Batina/Li ua/Wu/Kasahara, Applied Cryptography and Network Security Workshops, 2023, 67 (71).
88 Dazu allg. Chen/Lu/Kunpittaya/Luo, A Review of Zero Knowledge Proofs, S. 12.
89 Williams, Remote Voting in the Age of Cryptography MIT Computational Law Report, 5.12.2022, https://law.mit.edu/pub/remotevotingintheageofcryptography.
90 ElSheikh/Youssef/Hasan IEEE, TNSE 2025, 2566 (2576).
91 Sangraula/Adhikari Journal of The Institution of Engineers (India): Series B 2025, 1861 (1867 f.).
92 Jimmy/Rimba/Vincent/Purba/Darwin Teknika 2025, 433 (440).
93 Ernstberger/Chaliasos/Zhou/Jovanovic/Gervais Cryptology ePrint Archive 2024, 050, S. 7.

die Techniken daher als elementarer Baustein sicherer E-Voting-Systeme und liegen nahezu allen wissenschaftlich fundierten Systemen zugrunde.[94] So setzt etwa der ElectionGuard von Microsoft[95] ebenso auf sie wie das pilotierte blockchainbasierte Wahlformat der Schweizer Stadt Zug.[96]

2. Fehler- und Manipulationsanfälligkeit

Auch wenn digitale Wahlstrukturen die Geheimheit der Wahl gewährleisten, sind sie ihrem Wesen nach eine attraktive Zielscheibe unerlaubter Angriffe. Dritte können sich unerkannt in den Prozess einklinken. Das lässt sich weder punktuell noch flächendeckend vollständig ausschließen – schon deshalb, weil sich das Innenleben elektronischer Wahlgeräte nicht einsehen lässt. Einfache Mechanismen (zB ein Papierprotokoll) allein reichen nicht aus, um Fehler und Manipulationen zuverlässig zu detektieren.[97]

Moderne elektronische Wahlinstrumente sind technisch indes bereits deutlich ausgereifter als die Wahlcomputer zur Zeit des Wahlcomputer-Urteils des BVerfG im Jahr 2009. Davon profitieren auch die eingebundenen Risikomanagementstrukturen. Der schlichte Papier-Durchschlag des inneren Verarbeitungsvorgangs entspricht heutigen Standards nicht mehr. Unterdessen hat sich ein sicherheitstechnischer Quantensprung vollzogen: Die Architektur der Blockchain sichert Fehler- und Manipulationsfreiheit von innen heraus ab.[98] Nachvollziehbarkeit und Sicherheit gehen so Hand in Hand. Die kryptographische Verschlüsselung dient als Kontrollinstanz und beugt Fehlern sowie Manipulationen frühzeitig vor. Jede Stimme lässt sich mit einer kryptographischen Signatur versehen. Stimmen ohne gültige Signatur gelangen so gar nicht erst in die digitale Wahlurne.[99] Hat die Stimme einmal Eingang in die Blockchain-Kette gefunden, lässt sie sich nachträglich nicht mehr unbemerkt ändern oder löschen, ohne dass sich die gesamte nachfolgende Kette auflöst.[100] Die Blockchain ist damit faktisch unveränderlich.[101] Dezentrale Strukturen bieten Manipulationsversuchen kein zentrales Einfallstor. Selbst interne Angriffe lassen sich damit erheblich erschweren, wenn nicht sogar gänzlich ausschließen.[102] Indem die Blockchain die Datenhoheit auf mehrere Akteure aufteilt, wirkt sie gerade bei Personalrats-, aber auch Betriebsratswahlen, die ihrem Wesen nach unter der Infrastruktur des Dienstherrn bzw. Arbeitgebers ablaufen, überdies etwaigem Misstrauen der Beschäftigten entgegen.

Dezentrale Strukturen sind aber auch ihrerseits vielfältigen Sicherheitsrisiken ausgesetzt. Kryptographische Verfahren und Blockchain-Systeme sind in komplexe Software eingebettet. Systemfehler oder Sicherheitslücken lassen sich dadurch auf den ersten Blick nur schwer erkennen. Nutzen Angreifer diese aus, wiegen die Folgen umso schwerer. So kann sich der vermeintliche Schutzwall der Dezentralität auch als offene Flanke entpuppen. Gerade in kleinen Wahlumgebungen (wie bei Personalratswahlen) können sog. Mehrheitsangriffe die Dezentralisierung aushebeln.[103] Bei einem solchen Angriff bündelt der Angreifer mehr als 50 % der Rechenleistung der Blockchain. Damit überspielt er die anderen Beteiligten im dezentralisierten Netzwerk beim Abgleich der Ketten. Dieser Vorsprung erlaubt es ihm, Transaktionen zu verändern.[104] Ist ein solcher Angriff einmal geglückt, kehrt sich die Unveränderlichkeit der Blockchain gegen sie selbst: Die in die Kette eingeschriebene Manipulation lässt sich nur schwerlich wieder korrigieren.

Die Risiken, die kryptographische Verfahren und die Blockchain-Technologie bergen, lassen sich jedoch einhegen.[105] Die Informationstechnik hat vielfältige Maßnahmen entwickelt, um auftretende Fehler oder Manipulationen zu bereinigen.[106] Dafür eignen sich insbesondere sog. *Chameleon-Hashes*. Sie sind von vornherein darauf angelegt, sich nachträglich verändern zu lassen.[107] Soll eine Transaktion nicht nur eine andere Gestalt annehmen, sondern gänzlich verschwinden, können Rollback-Mechanismen die Kette in einen früheren Zustand zurückversetzen.[108] Damit nicht jeder Teilnehmer die Blockchain nach Belieben bricht oder verändert, sollten solche Kontroll- und Korrekturmaßnahmen nur einem engen Kreis von Personen vorbehalten bleiben.[109] Zusätzliche Sicherheit verheißt es, die Befugnisse nach dem Vieraugenprinzip als „Gesamthandsberechtigung“ oder in einem Stufenmodell auszugestalten. Änderungen an der Blockchain bleiben so dem Zugriff Einzelner entzogen. Sie lassen sich nur gemeinsam, als qualifizierte Mehrheit oder nach vorausgehenden Sicherheitsetappen (zum Beispiel einem Wahlprüfungsverfahren) von legitimierten Akteuren durchführen.[110] Die dezentrale Blockchain-Struktur sichert im Ergebnis das Wahlverfahren an mehreren Stellen zeitgleich und verhindert so Informationsverluste durch Manipulationsversuche.[111] Etablierte Blockchain-Systeme zeigen dadurch in der Praxis eine besondere Fehler- und Manipulationssicherheit.

3. „Ohne besondere technische Vorkenntnisse“

Ihre Kontrollfunktion bei Wahlen kann die breite Öffentlichkeit nur dann erfüllen, wenn diese Überprüfung keine besonderen technischen Vorkenntnisse erfordert. Obgleich der Öffentlichkeitsgrundsatz gebietet, das Wahlverfahren für jedermann nachvollziehbar auszugestalten,[112] verlangt er aber nicht, dass jeder Laie einen tieferen Einblick in das Systeminnere nehmen kann. Die eingesetzte Technik muss sich also nicht notwendigerweise so weit herunterbrechen lassen, dass die breite Masse sie versteht. Es reicht aus, dass sich Wahlablauf und Zusammensetzung des Wahlergebnisses nachvollziehen lassen und die Öffentlichkeit sie insoweit kontrollieren *kann*. Entscheidend sind geeignete Mittel, damit sich die technisch komplexen Vorgänge einfach einsehen lassen

94 Vgl. Berenjestanaki/Barzegar/El Ioini/Pahl Electronics 2024, 13:1, 17 (22, 26).
95 Benaloh/Naehring/Pereira/Wallach USENIX Association, Proceedings of the 33rd USENIX Conference on Security Symposium, 2024, 5485 (5486).
96 Rauschenbach/Stucki, Studie zum Einsatz der Blockchain-Technologie in der kantonalen Verwaltung, S. 29.
97 Vgl. II. 1.
98 Hackmann K&R 2019, 777 (780).
99 Buchmann/Roßnagel K&R 2009, 543 (547).
100 Im Allg. Noller/Reinhardt/Becker, Handbuch Philosophie der Digitalität, 2025, 1 (3).
101 BSI, Blockchain macht Daten praktisch unveränderbar, https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Technologien_sicher_gestalten/Blockchain-Kryptowaehrung/blockchain-kryptowaehrung_node.html.
102 Luxoft/Hochschule Luzern/Stadt Zug, Evaluation of the blockchain vote in the city of Zug, S. 1.
103 Vgl. Hackmann K&R 2019, 777 (778). Bei privater Blockchain-Struktur kann das geschützte Umfeld Angriffen entgegenwirken.
104 Statt vieler Eckert, IT-Sicherheit, 10. Aufl. 2018, S. 839.
105 Schlatt/Schweizer/Urbach/Fridgen, Blockchain: Grundlagen Anwendungen, Potenziale, S. 3.
106 Eine Übersicht über verschiedenste Ansätze bietet Richter Vidal/Ivaki/Laranjeiro IEEE, 10th Latin-American Symposium on Dependable Computing (LADC), 2021, 1.
107 Martini/Weinzierl NVwZ 2017, 1251 (1256).
108 BSI, Blockchain sicher gestalten, S. 63.
109 Vgl. Martini/Weinzierl NVwZ 2017, 1251 (1256 f.).
110 Vgl. Ruoti/Kaiser/Yerukhimovich/Clark/Cunningham Communications of the ACM 2020, 63:1, 46 (51). Die Wahlhelfer benötigen dafür keine besondere Fachkenntnis. Eine nutzerfreundliche Oberfläche erlaubt es ihnen, die Blockchain intuitiv zu bedienen.
111 Hackmann K&R 2019, 777 (780).
112 Mast JZ 2021, 237 (243).

und das notwendige Vertrauen in die Richtigkeit des Wahlergebnisses entsteht.

Der Öffentlichkeitsgrundsatz errichtet damit für technische Wahlmittel keine unüberwindbar hohen Hürden. Mit Blick auf die Stimmerfassung hätte es bereits für die Wahlcomputer der ersten Stunde ausgereicht, wenn diese ein Papierprotokoll ausgegeben hätten. Mit dem physischen Doppel hätte der Wähler – auch ohne den inneren Datenverarbeitungsvorgang zu verstehen – kontrollieren können, ob das System seine Stimme zutreffend registriert und entsprechend in das Wahlergebnis übernimmt.[113] Diese verfassungsrechtlich gebotene „Frontend"-Kontrolle bewältigen moderne technische Systeme mühelos.

Die eigentliche Engstelle liegt anderswo, nämlich am Anfang der Kette: Der Wähler muss ohne vertiefte Fachkenntnisse erkennen können, dass das System seine Stimmabgabe inhaltlich übernimmt. Auch dies lässt sich aber sicherstellen: Die Unveränderlichkeit der Blockchain sichert ab, dass eine einmal zutreffend erfasste Stimme sich auch unverfälscht lückenlos in die Wahl-Kette einreiht und alle Stimmen zutreffend in das Wahlergebnis eingehen. Den Blick in die Blockchain eröffnen sog. *Explorer*. Diese Analyse-Tools erlauben es dem Einzelnen, eine Blockchain nach beliebigen Merkmalen zu durchforsten.[114] Ihre Nutzeroberfläche operiert ähnlich wie bekannte Suchmaschinen. Auch ohne Fachkenntnisse lassen sie sich im Idealfall leicht bedienen.[115] Mit den passenden Sicherheitseinstellungen unterlegt, eröffnen sie den Blick auf die gesamte Kette und die Möglichkeit einer lückenlosen unabhängigen Prüfung, ohne sensible Informationen offenzulegen.[116]

Die Befürchtung, digitale Wahlformate ließen sich schon wegen ihrer technischen Komplexität nicht rechtskonform ausgestalten, bewahrheitet sich daher nicht. Die Öffentlichkeit muss sich nicht in einen Zirkel von IT-Fachleuten verwandeln, um ihre Kontrollfunktion zu erfüllen. Die notwendige Kontrollmöglichkeit eröffnen nutzerfreundliche Tools, die keine spezifischen Fachkenntnisse erfordern, grundsätzlich auch für Laien.

4. Verbleibende Risiken

So sehr die Blockchain-Technologie als dezentrales, unveränderliches Kassenbuch abgegebene Stimmen durchgängig verifizierbar macht und die homomorphe Verschlüsselung die Auszählung der Stimmen ermöglicht, ohne deren Geheimhaltung zu gefährden: Absolute Sicherheit können auch sie nicht verbürgen. Die Risiken und Herausforderungen lauern vorrangig jenseits des technischen Wirkkreises der Blockchain und der homomorphen Verschlüsselung.[117]

Denn die Technologien können ihre Funktion nur dann sachgerecht erfüllen, wenn sie in eine ausreichend stabile und sichere Netzwerkstruktur eingebunden sind. Die Blockchain wie die homomorphe Verschlüsselung sind äußerst rechenintensiv.[118] Wenn Millionen Wahlberechtigte digital wählen, kann dies zu Performance-Überforderungen des Systems und daher zu Ausfällen führen. Flächendeckende Angriffe auf die Netzstruktur (sog. DDoS-Angriffe[119]) können das Risiko eines Systemzusammenbruchs zusätzlich befeuern.[120]

Selbst wenn die Architektur die notwendigen Rechenkapazitäten bereitstellt, vermag die dezentrale Blockchain-Infrastruktur nicht zu verbürgen, dass es immer – wie im Wahllokal – die stimmberechtigte Person ist, welche die Stimme abgibt, und dies unbeobachtet sowie frei von äußerem Druck und Beeinflussung durch Familienmitglieder, Erpressungstäter etc. erfolgt.[121] Das kann allerdings auch die – verfassungsrechtlich zulässige[122] – Briefwahl ebenso wenig.

Mit der Abkehr von Stift und Papier gesellt sich aber eine weitere Risikodimension hinzu: Anders als dort kann die Online-Wahl nicht garantieren, dass das Endgerät des Wählers (namentlich sein Smartphone, Tablet oder PC) frei von Schadsoftware ist.[123] Stimmen lassen sich außerhalb der digitalen Wahlumgebung unbemerkt manipulieren, bevor sie verschlüsselt in die digitale Wahlurne eingehen.[124] Das Risiko, dass Dritte Phishing-Angriffe unternehmen und kryptographische Schlüssel in großem Maßstab abgreifen, lässt sich nicht vollständig eliminieren.[125] Unabhängig von der Sicherheitsarchitektur des Wahlsystems öffnet die Endeinrichtung des Wählers damit ein Einfallstor für Wahlmanipulationen.

Heute noch nicht im Detail absehbare künftige technische Entwicklungen bergen überdies weitere Risiken: Quantencomputer werden alsbald gängige Verschlüsselungen aufbrechen.[126] Sie stellen dann einen Generalschlüssel bereit, der Einblick in alle Inhalte vermittelt. Heutige Verschlüsselungsverfahren sind daher nicht auf Dauer gegen Entschlüsselung geschützt. Für die Richtigkeit eines einmal festgestellten Wahlergebnisses ist das unschädlich – anders jedoch für die Geheimheit einer einmal abgegebenen Stimme. Mögliche „Harvest now, decrypt later"-Angriffe gefährden die Vertraulichkeit von Wahlen und damit die Stimmabgabe bereits, bevor die Entschlüsselung massentauglich wird. Geboten sind daher Post-Quanten-kryptographische homomorphe Verschlüsselungsverfahren, die auch künftigen Angriffen voraussichtlich standhalten.[127] Verbleibenden Risiken wirken zwei Vorkehrungen entgegen: zum einen die Schlüsselkomponenten auf verschiedene unabhängige Institutionen zu verteilen, zum anderen gesetzliche Löschungsmechanismen nach rechtsverbindlicher Feststellung des Wahlergebnisses vorzusehen.

Allein, dass ein Angriff theoretisch möglich ist, sagt aber noch nichts darüber, ob und in welcher Form er tatsächlich

113 S. bereits II. 1.
114 Dhillon/Metcalf/Hooper, AI Frameworks Enabled by Blockchain, 2025, S. 8.
115 Hünseler/Lemke-Rusk/Pöll/Stoppenbrink/Boden/Jakobi/Stevens ua, Verbraucherdatenschutz, 2021, 1 (20); ähnl. Mast JZ 2021, 237 (238).
116 Abed/Al-Zoubi/Alayan/Alshboul Cluster Computing 2024, 4635 (4644 ff.). Beschränkt auf die eigene Stimme Hjálmarsson/Hreiðarsson/Hamdaqa/Hjálmtýsson IEEE, 11th International Conference on Cloud Computing (CLOUD), 2018, 983 (985); Fatih/Arezki/Gadi iJIM 2023, 49 (56). Nach Berechtigung differenzierend Singh/Sinha Multimedia Tools and Applications 2024, 58875 (58883).
117 Vgl. BSI, Blockchain sicher gestalten, S. 52 f.
118 Shaikh/Wiil/Ebrahimi/Memon IJNDC 2025, 14:1, 4, S. 10 ff. für verschiedene Konsensmechanismen; Damie/Pop/Posthuma, Energy Consumption of TLS, Searchable Encryption and Fully Homomorphic Encryption, v3 S. 14 für die voll-homomorphe Verschlüsselung im Vergleich zu anderen Verschlüsselungsmethoden.
119 Distributed Denial of Service-Angriffe sind gezielte Cyberattacken, die ein System, Server oder Netzwerk mit Datenmengen oder Anfragen überlasten, um es stark zu verlangsamen oder zum Absturz zu bringen.
120 Zhang/Wang/Xiong IJIS 2020, 323 (331, 335 f.).
121 Bretthauer KritV 2021, 3 (27).
122 BVerfGE 59, 119 (126 ff.) = NJW 1982, 869 (870).
123 Beckert/Budurushi/Grunwald/Krimmer/Kulyk/Küsters/Mayer/Müller-Quade/Neumann/Volkamer, Aktuelle Entwicklungen im Kontext von Online-Wahlen und digitalen Abstimmungen, S. 15.
124 Vgl. Alshehri/Baza/Srivastava/Rajeh/Alrowaily/Almusali Applied Sciences 2023, 13:2, 1096, S. 1.
125 BSI, Blockchain sicher gestalten, S. 55. Eine umfassende Liste weiterer Angriffsformen findet sich bei BSI, Technische Richtlinie TR-03169, Version 1.1, S. 10.
126 Ab wann damit zu rechnen ist, stößt auf unterschiedliche Einschätzungen. Die geschätzte Zeitspanne reicht von wenigen Jahren bis zu mehreren Jahrzehnten, vgl. Schärer/Comuzzi Quantum Machine Intelligence, 2023, 5:1, 19, S. 10.
127 Zum aktuellen Entwicklungsstand quantensicherer homomorpher Verschlüsselung grundlegend Bhoi/Arakala/Cormen/Rao Cryptography 2025, 9:2, 31, S. 1.

stattfindet. Entscheidend ist, mit welcher Wahrscheinlichkeit und in welchem Ausmaß sowie mit welchen Auswirkungen die Angriffe zu erwarten sind.[128] Der Blick auf den Markt für Cybercrime-Produkte zeigt, dass Angriffe keine umfassenden finanziellen Ressourcen oder besonderen technischen Fähigkeiten erfordern: Eine breite Masse an technischen Angriffsmöglichkeiten – einschließlich DDoS-Attacken – lässt sich schon für unter 100 EUR erwerben bzw. buchen.[129] KI-basierte Phishing-Angriffe sind sogar noch günstiger, kosten nur wenige Cent pro Angriff und verheißen zugleich höhere Erfolgsquoten als klassisches Massen-Phishing.[130] Je größer die Zahl der Wähler und je bedeutsamer die Wahl für politische Wegentscheidungen ist, umso leichter lassen sich Angriffe skalieren, umso schwerer lassen sie sich auf einzelne Wählergruppen zurückverfolgen und umso sprunghafter steigt das Manipulationsrisiko der Online-Wahl.[131] Bundestags-, Landtags- und Kommunalwahlen sind daher gegenwärtig online noch nicht hinreichend sicher abbildbar.

In kleinräumigen Kontexten, wie etwa bei Hochschul-, Betriebsrats- oder Personalratswahlen, sind die politischen Wirkkräfte der gewählten Institutionen schwächer und dementsprechend auch der Gewinn, den Angreifer erzielen, bzw. die Schäden, die sie verursachen können. Der Wahlkörper ist klar abgegrenzt. Die Identität der Wähler zu ermitteln, ist typischerweise mühevoll und ressourcenintensiv. Der technische, organisatorische und finanzielle Aufwand, den ein wirksamer Angriff erfordert, steht dann regelmäßig in keinem Verhältnis zu den Erfolgen, die er im besten Fall erreichen kann. Das senkt die zu erwartende Motivation der Angreifer sowie ihre Bereitschaft, Expertise und Ressourcen in die Manipulation zu investieren. Kleineren Angriffen lässt sich schon mit überschaubar aufwändigen Sicherheitsmaßnahmen begegnen.[132] Etablierte, auf Online-Wahlen zugeschnittene Sicherheitstechniken bieten risikoadäquaten Schutz: Moderne Captcha-Mechanismen verhindern Phishing,[133] Firewalls sowie VPN-Zugänge gewährleisten im Grundsatz sichere Übertragungswege.[134] Die Bandbreite implementierbarer Sicherheitstechniken ist ebenso vielfältig wie ihre mögliche Feinjustierung. Das nötige Schutzniveau lässt sich so passgenau an die Gefahrenprognose angleichen.

Solche Schutzvorkehrungen können zwar auch versagen. Digital durchgeführte Angriffe hinterlassen aber Spuren und lassen sich – gegebenenfalls ex post – detektieren.[135] Online-Wahlen lassen sich mit überschaubarem Aufwand und kostengünstiger als klassische Wahlformate wiederholen, ohne zwangsläufig das Vertrauen in grundlegende demokratische Institutionen zu erschüttern.

Ist die äußere Struktur der Online-Wahl hinreichend robust ausgestaltet, überwiegen die Vorteile für die Öffentlichkeit und Allgemeinheit der Wahl (insbesondere mit Blick auf die Chance auf eine höhere Wahlbeteiligung) die Risiken.[136] Anders als analoge Wahlen generiert ein kryptographisch abgesichertes Online-System auch keine Auszählungsfehler oder Stimmverluste auf dem Postweg. Es empfiehlt sich, für digitale Wahlformate Reallabore aufzubauen, in denen sich Online-Wahlen mit BSI-zertifizierter Software unter kontrollierten und regulierten Testbedingungen erproben und validieren lassen.

IV. Rechtliche Spielräume im Labor des Digitalrechts am Beispiel der Experimentierklausel des Art. 56 S. 1 Nr. 3 BayDiG

Legislatorisch können Experimentierklauseln eine Digitalisierung nicht-politischer Wahlen ermöglichen und damit die Tür zur praktischen Umsetzung aufstoßen. In Bayern erlaubt das Digitalisierungsgesetz „[…] Abweichungen von […] sonstigen landesgesetzlichen Zuständigkeits- und Formvorschriften“, um „digitale[.] Verwaltungsinfrastrukturen“ einzuführen und fortzuentwickeln (Art. 56 S. 1 Nr. 3 BayDiG).[137] Nach dem Willen des Landesgesetzgebers soll die Vorschrift weite Spielräume eröffnen und damit die nötige Flexibilität schaffen, um neue Technologien zu erproben.[138]

Ob die Experimentierklausel sich auch auf Personalratswahlen erstreckt, ist aber alles andere als klar. Denn diese entsprechen nicht klassischen Mustern administrativen Handelns (1.). Selbst wenn sie sich der Verwaltungsinfrastruktur zuordnen lassen, muss es sich bei der Vorgabe „Stimmzettel“ (§ 14 II 1 WO-BayPVG) auch um eine Formvorschrift iSd Art. 56 S. 1 Nr. 3 BayDiG handeln (2.). Um die Vereinfachung durch Digitalisierung auf ein sachgerechtes Maß zu begrenzen, zieht die Norm zudem weitere Schranken ein, insbesondere einen Erforderlichkeitsvorbehalt, dem die Befreiung vom Wahlzettel genügen muss (3.). Eine legalisierende Rechtsverordnung muss überdies hohen inhaltlichen Anforderungen genügen (4.).

1. Personalvertretung als Element der Verwaltungsinfrastruktur?

Dass sich der Personalrat als Teil der Verwaltungsinfrastruktur iSd Art. 56 S. 1 BayDiG begreifen lässt, drängt sich nicht unmittelbar auf. Was unter diesen Begriff fällt, definiert das Gesetz nicht. Es setzt ihn vielmehr voraus (so etwa in Art. 36 f. BayDiG). Nach seinem Sinn fungiert er als Sammelbezeichnung, die sämtliche organisatorischen, technischen und rechtlichen Rahmenbedingungen der Verwaltung umfasst.

Der Personalrat ist zwar weder eine technische Verwaltungsinstanz noch eine eigenständige Behörde. Darauf ist der Topos „Verwaltungsinfrastruktur“ aber auch nicht begrenzt. Der Personalrat repräsentiert als Institution der Dienststellenverfassung einen integralen Bestandteil der Binnenorganisation. Das umfasst zwangsläufig auch seine Errichtung, also seine Wahl.[139] Er ist damit als Interessenvertretung im öffentlichen Dienst Teil der Verwaltungsinfrastruktur.

Die Experimentierklausel beschränkt sich nicht auf Digitalisierungstests für Handlungen in einem Verwaltungsverfahren, das auf eine Sachentscheidung zielt. Die Stoßrichtung des Art. 56 BayDiG reicht deutlich weiter. Ausweislich der Gesetzesbegründung zielt er darauf ab, „neue und innovative E-Government-Lösungen“ zuzulassen.[140]

128 Vertiefend hierzu Maulana/Putra/Yasa IEEE, 9th International Conference On Electrical, Electronics And Information Engineering (ICEEIE), 2025, 431 (432 f.).
129 Georgoulias/Yaben/Vasilomanolakis ACM, ARES '23: Proceedings of the 18th International Conference on Availability, Reliability and Security, 2023, 106, S. 6 ff.
130 Heiding/Lermen/Kao/Schneier/Vishwanath, Evaluating Large Language Models' Capability to Launch Fully Automated Spear Phishing Campaigns: Validated on Human Subjects, S. 8 ff.
131 Vgl. BSI, Technische Richtlinie TR-03169, Version 1.1, S. 9.
132 BSI, Technische Richtlinie TR-03169, Version 1.1, S. 9.
133 Reddy/Vani IJARCCE 2013, 3434 (3435).
134 Harris, Internet of Things: Considerations and Recommendations for Internet-Based Voting Equipment, S. 6.
135 Vgl. bereits III. 1., 2.
136 Ähnl. BSI, Technische Richtlinie TR-03169, Version 1.1, S. 9.
137 Vergleichbare Regelungen bestehen in § 17 I 1 Nr. 3 BbgEGovG, § 19 S. 1 Nr. 3 HEGovG, § 25a I Nr. 3 NRWEGovG, § 27 S. 1 Nr. 3 E-GovG SL, § 20 SächsEGovG, § 25 Nr. 3 EGovG LSA.
138 BayLT-Drs. 18/19572, 36.
139 Richardi/Dörner/Weber/Annuß/Richardi, 6. Aufl. 2024, BPersVG Einl. Rn. 75 ff.
140 BayLT-Drs. 18/19572, 36.

„E-Government" erschöpft sich nicht darin, etablierte Handlungsmodelle der Verwaltung zu elektronifizieren. Es umschließt vielmehr sämtliche administrativen Prozesse, die sich digital abbilden lassen. Sein Leitbild zielt gerade darauf ab, etablierte Organisations- und Verfahrensstrukturen zu hinterfragen und aufzubrechen.[141] Die Experimentierklausel soll also nicht nur ermöglichen, Vorbereitungsmaßnahmen zu transformieren. Sie soll die gesamte Verwaltungsstruktur für neue Technologien öffnen. Diese weitreichende Zielsetzung des Landesgesetzgebers unterstreicht auch Art. 2 S. 2 Nr. 12 BayDiG: Die Norm erstreckt Maßnahmen, welche die Digitalisierung fördern, auf die gesamte „Verwaltung und den Ausbau digitaler Verwaltungsangebote". Sie beschränkt sich insbesondere nicht auf Verfahrenshandlungen. Auch Art. 56 BayDiG selbst verdeutlicht, dass das übergeordnete Digitalisierungsziel weit gesteckt ist: Art. 56 S. 1 Nr. 3 BayDiG erlaubt, mit allen „sonstigen landesgesetzlichen […] Formvorschriften" zu experimentieren. Der Auffangtatbestand erstreckt die Digitalisierung der Verwaltung damit – auch, aber nicht nur – auf das Handeln nach außen. Er ermöglicht ebenso, von rein innerbehördlichen Formvorschriften zu befreien. Er erfasst mithin das allgemeine Verwaltungshandeln und die einschlägigen Formvorschriften für das Wahlprozedere gleichermaßen.

2. Wahlzettel als Formvorschrift

Die Experimentierklausel des Art. 56 S. 1 Nr. 3 BayDiG gestattet ausschließlich, von Zuständigkeits- und Formvorschriften, nicht aber von materiellem Recht abzuweichen. Wer das Wahlverfahren formal umgestaltet, berührt damit aber grundsätzlich auch den Öffentlichkeitsgrundsatz als materielle Vorgabe: „Klick" statt „Kreuz" ändert nicht nur das Wahlformat. Es steckt zugleich den Rahmen des Öffentlichkeitsgrundsatzes neu ab.

§ 14 II 1 WO-BayPVG gewährleistet diesen – entsprechend dem impliziten Verständnis des BayPVG – de lege lata durch einen Rekurs auf die Papierform: Wahlberechtigte müssen einen Stimmzettel abgeben, um ihr Wahlrecht auszuüben.

Abstriche auf formeller Ebene gehen im Zweifel also auch mit Abstrichen beim dahinterstehenden materiell-rechtlichen Verfassungsprinzip einher. Dass eine Formvorschrift auch materielle Implikationen zeitigt, lässt ihren Charakter jedoch unberührt. Denn Form- und Verfahrensvorschriften erschöpfen sich nicht in einem Selbststand. Sie sollen typischerweise materielle Rechtspositionen absichern.[142]

Am Charakter der Regelung des § 14 II 1 WO-BayPVG als Formvorschrift ändert sich jedenfalls dann nichts, wenn sich der übergeordnete Schutzgehalt der Öffentlichkeit der Wahl auch ohne die gesetzlich vorgegebene Form sichern lässt. Mit anderen Worten: Kann der Öffentlichkeitsgrundsatz seine Funktion auch entfalten, wenn moderne digitale Wahlformate zum Einsatz kommen, bleibt dies auf seinen materiellen Gehalt ohne Einfluss. Hinter der Vorgabe „Stimmzettel" steckt eine Formvorschrift, die das Verfassungsrecht nicht zwingend verlangt. Denn auch andere Formate als die Papierform können gewährleisten, dass sich das Wahlverfahren nach den Vorgaben des Öffentlichkeitsgrundsatzes kontrollieren lässt.[143] Bei ihr handelt es sich nur um eine von mehreren denkbaren Gestaltungsvarianten. Der analoge Wahlzettel erfüllt lediglich eine „dienende Funktion" als physischer Träger der Wählerstimme. § 14 II 1 WO-BayPVG ist damit offen dafür, digitale Wahlzettel für die Personalratswahl „zur Erprobung […] des Schriftformersatzes" (Art. 56 S. 1 Nr. 3 BayDiG) einzusetzen.

Art. 56 S. 1 Nr. 3 BayDiG gestattet aber nicht, pauschal von *jeglicher* Zuständigkeits- oder Formvorschrift abzuweichen. Er benennt ausdrücklich und abschließend, welche Zuständigkeits- und Formvorschriften erfasst sind. Dazu gehören insbesondere landesgesetzliche Vorschriften, soweit dies „zur Erprobung neuer digitaler Formen des Schriftformersatzes" oder „der Übermittlung […] von […] Erklärungen […] erforderlich ist".

§ 14 II 1 WO-BayPVG ist zwar keine formell-gesetzliche Vorschrift. Seinem Sinn nach erfasst Art. 56 S. 1 Nr. 3 BayDiG aber zum einen – erst recht – landesrechtliche Vorschriften, die unterhalb des formellen Landesgesetzes stehen; zum anderen geht das BayPVG von der Papierform als ungeschriebenem Grundsatz aus. Dass § 14 II 1 WO-BayPVG nicht ausdrücklich von „Schriftform" spricht, ist unschädlich. Das öffentliche Recht kennt – anders als das Zivilrecht (vgl. va § 126 BGB) – kein einheitliches Bild der Schriftform.[144] Dem offenen Begriffsverständnis verleihen die jeweiligen Fachgesetze vielmehr inhaltlich eigenständige Konturen.[145] Auch dort, wo der Gesetzgeber andere Begrifflichkeiten (zB „Niederschrift") verwendet, kann sich dahinter das tradierte Bild von Stift und Papier verbergen.[146] Im Lichte der Wahlrechtsgrundsätze – insbesondere der Geheimheit – darf das Format des Stimmzettels bspw. weder eine Unterschrift noch sonst ein Merkmal tragen, das den Wähler erkennen lässt.[147] Zugleich verfestigt das Dokument die Stimmabgabe (Perpetuierungsfunktion) und weist diese nach (Beweisfunktion). Der Stimmzettel erfüllt damit wesentliche Funktionen, die sonst die klassische Schriftform übernimmt.[148] Er errichtet eine wahlspezifische Schriftlichkeit.[149] Der Wahlzettel verkörpert daher nichts anderes als eine besondere Form, die als Teil der Experimentierklausel grundsätzlich der Abweichung zugänglich ist.

3. Inhaltliche Voraussetzungen, insbesondere Erforderlichkeitsvorbehalt

Art. 56 S. 1 Nr. 3 BayDiG erteilt keine *carte blanche*, mit geltenden Formvorschriften zu brechen. Eine Ausnahmegenehmigung ist vielmehr sachlich, räumlich sowie zeitlich zu begrenzen; sie muss zudem erforderlich sein, um neue digitale Formen des Schriftformersatzes bzw. der Übermittlung von Erklärungen zu erproben (Art. 56 S. 1 Nr. 3, S. 2 BayDiG).

Der Erforderlichkeitsvorbehalt etabliert keinen Suchmechanismus nach einem milderen, gleich geeigneten Mittel[150] zur anvisierten Technik. Die Befreiung vom Schriftformerfordernis muss lediglich das erforderliche Mittel sein, um die ausgewählte Technik erproben zu können. Es reicht daher bereits aus, dass keine schonendere Alternative als die Ausnahme von der Formvorschrift zur Verfügung steht, um gleichermaßen wirksam zu experimentieren.

141 Schoch/Schneider/Hornung, 7. EL 2025, VwVfG § 3a Rn. 2, 4.
142 Vgl. Abraham MMR 2020, 530 (532).
143 S. bereits II. 1.
144 Abraham MMR 2020, 530 (531).
145 Stelkens/Bonk/Sachs/Schmitz/Prell, 10. Aufl. 2023, VwVfG § 3a Rn. 17.
146 Abraham MMR 2020, 530 (531).
147 Huber/Voßkuhle/Müller/Drossel, 8. Aufl. 2024, GG Art. 38 Rn. 100. Zu den Möglichkeiten einer geheimen digitalen Signatur etwa Bremke LKV 2004, 102 (105).
148 Zusammenfassend NK-VwVfG/Schulz, 3. Aufl. 2025, VwVfG § 3a Rn. 108.
149 Vgl. Richardi/Dörner/Weber/Annuß/Dörner, 6. Aufl. 2024, BPersVG § 19 Rn. 5; aA wohl Bremke LKV 2004, 102 (105).
150 Zur Erforderlichkeit im Allgemeinen statt vieler Dürig/Herzog/Scholz/Grzeszick, 109. EL 2026, GG Art. 20 Rn. 115 ff.

§ 14 II 1 WO-BayPVG schreibt den Wahlzettel bei den bayerischen Personalratswahlen als zwingendes Erfordernis vor, um das Wahlrecht ausüben zu können. Digitale Personalratswahlen ersetzen den analogen Stimmzettel. Um Pilotprojekte zur digitalisierten Personalratswahl im vollen Umfang praxisgerecht zu erproben, sind Ausnahmen vom Schriftlichkeitsgebot daher unumgänglich. Allenfalls die Möglichkeit, digitale Stimmabgaben *zusätzlich* zum Stimmzettel auf Papier zu implementieren,[151] ist eine schonendere Alternative, um Digitalisierungspotenziale auszuschöpfen. Die digitale Wahl ist aber ohnedies nicht als einzige, sondern als ergänzende Möglichkeit konzipiert, die eigene Stimme abzugeben. Die Befreiung vom Schriftformerfordernis entpuppt sich daher als erforderlich, um mit digitalen Wahlformaten experimentieren zu können.

4. Anforderungen an die Rechtsverordnung

Soweit Art. 56 S. 1 Nr. 3 BayDiG es gestattet, Online-Wahlen zum Personalrat zu erproben, muss eine legalisierende Rechtsverordnung die Rahmenbedingungen näher ausformen. Diese erlässt das Staatsministerium für Digitales im Einvernehmen mit der Staatskanzlei und den fachlich betroffenen Ressorts (Art. 56 S. 1 BayDiG).

Ob das Verfassungsrecht es gestattet, eine für die demokratische Ordnung wesentliche Frage in Gestalt einer Rechtsverordnung zu beantworten, ist damit allerdings nicht gesagt. Immerhin stehen demokratische Mitwirkungsrechte als grundrechtsgleiche Rechte[152] „im Feuer". In der parlamentarischen Demokratie bleiben wesentliche Grundentscheidungen der Volksvertretung als Gravitationszentrum des politischen Willensbildungssystems vorbehalten.[153] Das gilt auch für Wahlen unterhalb der Legitimationsebene „Bundestag, Landtag und Gemeinderat".

Für den Einsatz von Wahlcomputern steckte das BVerfG in seiner Entscheidung bereits den Spielraum des Gesetzgebers ab,[154] in dem er Regelungsbefugnisse an die Exekutive weiterreichen darf: „Einzelheiten dürfen im Wege einer Rechtsverordnung […] geregelt werden".[155] Es greift also kein *absoluter* Parlamentsvorbehalt.[156] „[D]ie Gestaltung der technischen Aspekte des Wahlvorgangs […] und damit die Entscheidung über einen Einsatz von Wahlgeräten und die Festlegung der näheren Voraussetzungen für deren Einsatz"[157] muss aber in den Händen des parlamentarischen Gesetzgebers verbleiben. Er ist es, der die Grundentscheidung über das „Ob" technischer Wahlformate zu treffen hat, bevor er die Detailfragen der Exekutive anvertrauen darf.

Deshalb steht es dem Verordnungsgeber auch nicht frei, Online-Personalratswahlen auf der Grundlage der allgemeinen Wahlordnungsermächtigung (Art. 94 BayPVG bzw. § 129 BPersVG) einzuführen. Diese umschließt zwar auch „die Stimmabgabe" (Art. 94 II Buchst. e BayPVG, § 129 Nr. 5 BPersVG) sowie „die Feststellung des Wahlergebnisses" (Art. 94 II Buchst. f BayPVG, § 129 Nr. 6 BPersVG). Ob online oder per Stift abgestimmt wird, ist aber keine technische Detailfrage. Der Gesetzgeber hat (wie bspw. in § 35 BWahlG und § 56 III SGB IV) die Grundentscheidung für Online-Wahlen selbst zu treffen. Bislang gehen das BayPVG und das BPersVG implizit von einer Papierwahl aus. Das macht insbesondere die Vorschrift § 14 II 1 WO-BayPVG deutlich: Diese gibt vor, den Stimmzettel vor dem Einwurf in die Urne zu falten.[158]

Wenn der Exekutive der Weg zu Online-Personalratswahlen über die allgemeine Verordnungsermächtigung des Personalvertretungsgesetzes versperrt ist, stellt sich umso mehr die Frage, ob Art. 56 S. 1 Nr. 3 BayDiG diesen ebnen kann. Denn auch er mündet im Ergebnis in eine Rechtsverordnung, welche die Wahl zulässt. Es besteht aber ein wichtiger Unterschied: Art. 56 S. 1 Nr. 3 BayDiG ermächtigt nicht dazu, dauerhaft vom gesetzlichen Grundmodell abzuweichen. Er öffnet als Experimentierklausel nur ein befristetes Erprobungsfenster. Die Maßnahme muss zwingend sachlich, räumlich und zeitlich begrenzt („höchstens fünf Jahre" – Art. 56 S. 2 BayDiG) erfolgen. Das Digitalgesetz formuliert bewusst die Leitentscheidung, die gesamte Verwaltung – einschließlich der Wahlen des Personalrats –[159] innovativen technischen Lösungsansätzen zu öffnen. Ob der Gesetzgeber bei Erlass des Art. 56 S. 1 Nr. 3 BayDiG auch Abweichungen von der Papierwahl erfassen wollte oder ob er vielmehr lediglich an Abweichungen von klassischen Formvorschriften gedacht hat, lässt sich hinterfragen. Immerhin möchte er aber die Vorschrift generell als Innovationsmotor für die Digitalisierung verstehen und in begrenztem Umfang Abweichungen von gesetzlichen Grundentscheidungen experimentell zulassen. Dies ist die Mission einer zeitlich begrenzt zugelassenen Online-Personalratswahl. Mit dem Parlamentsvorbehalt ist das noch vereinbar.

Die Rechtsverordnung muss aber die Ausnahme, die sie befristet erteilt, hinreichend bestimmt bezeichnen. Sie muss insbesondere abstecken, inwieweit die Dienststellen – sachlich und räumlich begrenzt – von den landesgesetzlichen Vorschriften abweichen dürfen (Art. 56 S. 1 Nr. 3 BayDiG).[160] Ihr Regelungsgehalt darf sich daher nicht darauf beschränken, den sachlich-räumlichen Bereich der Befreiung einzugrenzen. Sie muss das Pilotprojekt auch inhaltlich so konkret vorzeichnen, dass sie den Dienststellen klare Handlungsmaßstäbe an die Hand gibt und die zuständigen Verwaltungsgerichte eine digitale Personalratswahl nachträglich an diesen Maßstäben überprüfen können.[161] Zulassen sollte die Rechtsverordnung insbesondere allein BSI-zertifizierte Software.

Weitere Anhaltspunkte, welche konkreten inhaltlichen Vorgaben die zu erlassende Rechtsverordnung etablieren könnte, liefert das Sozialwahlrecht. Dort hatte der Bundesgesetzgeber schon früh ausdifferenzierte Vorgaben für Online-Wahlen getroffen. Die §§ 194a–d SGB V aF legten die Grundlage dafür, bei den Sozialversicherungswahlen der gesetzlichen Krankenkassen im Jahr 2023 im Rahmen eines Modellprojekts elektronische Wahlverfahren via Internet durchzuführen. Neben Vorgaben zur Zulässigkeit dieses Pilotprojekts zurrten die Vorschriften auch fest, wie die Wahl abläuft und wie die Wahlberechtigten ihre Stimme abgeben (§ 194b SGB V aF). Sie verlangten technische und organisatorische Vorkehrungen (§ 194c SGB V aF), die das Bundesministerium für Gesundheit in einer Rechtsverordnung nach den Anforderungen des § 194c I 2 Nrn. 1–7 SGB V aF inhaltlich konkretisieren sollte. Diese reichten von grundlegenden technischen Vorgaben (Nr. 1) über Vorgaben für

151 Zu derartigen Vorschlägen bereits II. 1.
152 BVerfGE 123, 267 (328 ff.) = NJW 2009, 2267 (2268).
153 BVerfGE 49, 89 (127) = GewArch 1979, 53 = BeckRS 1978, 109125.
154 Hierzu bereits II. 3.
155 BVerfGE 123, 39 (71) = NVwZ 2009, 708 (710).
156 Vgl. Stern/Sodan/Möstl StaatsR/Kau, 2. Aufl. 2022, § 41 Rn. 44.
157 BVerfGE 123, 39 (71) = NVwZ 2009, 708 (710).
158 Auf Bundesebene zeichnet sich ein ähnliches Bild: § 15 II 1 WO-BPersVG verlangt die Stimmabgabe „in einem Wahlumschlag", was einen physischen Stimmzettel impliziert.
159 Vgl. IV. 1.
160 Dürig/Herzog/Scholz/Grzeszick, 109. EL 2026, GG Art. 20 Rn. 58 ff., 67.
161 Dürig/Herzog/Scholz/Grzeszick, 109. EL 2026, GG Art. 20 Rn. 58.

die Wahlvorbereitung und -durchführung (Nr. 3) bis hin zu den Kommunikationswegen im Krisenfall (Nr. 7). Eine wichtige Orientierungslinie für die inhaltlichen Vorgaben, Maßnahmen und Verfahren zeichneten die (technischen) Richtlinien und sonstigen Sicherheitsanforderungen für Online-Wahlen sowie Online-Wahlprodukte.[162] Diese Anforderungen hat der Bundesgesetzgeber nach Ende des Modellprojektes im Kern in die gemeinsamen Vorschriften für die Sozialversicherung integriert (insbesondere § 54 IV, § 56 III SGB IV).[163]

V. Fazit – wie viel Vertrauen verdient die Online-Wahl?

Wahlen sind das Hochamt der Demokratie. In ihrer Liturgie zelebriert das Gemeinwesen die Staatswillensbildung in einem pluralistischen Verfahren, an dessen Ende ein aus einzelnen Stimmen verdichtetes Ergebnis steht. Diese Aggregation lebt davon, dass die Wahlberechtigten auf den ordnungsgemäßen Ablauf und die Richtigkeit des Wahlergebnisses vertrauen können. Das setzt voraus, dass die Öffentlichkeit alle wesentlichen Schritte der Wahl überprüfen kann. Der Gesetzgeber muss dafür sorgen, dass sich das Wahlverfahren auch ohne besondere Vorkenntnisse überprüfen lässt, und zugleich substanzielle Fehler- und Manipulationsrisiken ausschließen.

Der klassische Wahlzettel erfüllt die Anforderungen des Öffentlichkeitsgrundsatzes bruchfrei. Die aufmerksame Öffentlichkeit kann ihm auf seinem Weg folgen – von der Aushändigung über die Wahlkabine und den Weg der Stimme in die Wahlurne bis zum Strich auf der Zählliste.

Technische Wahlmittel entziehen sich dieser offenen Beobachtung und treten damit in ein Spannungsverhältnis zum Grundsatz der Öffentlichkeit. So wenig sich die Verfassung neuen digitalen Wahlverfahren gänzlich verschließt, so sehr errichtet sie hohe Nachvollziehbarkeitshürden. An ihnen sind die Bemühungen, Wahlen zu digitalisieren, bislang weitgehend abgeprallt. Denn je fehler- und manipulationsanfälliger die technischen Systeme sind, desto mehr schwindet das Vertrauen darin, dass das ermittelte Wahlergebnis richtig ist.

Der technische Fortschritt macht rechtliche Hürden für Online-Wahlen immer leichter überwindbar. Die Blockchain-Technologie kann als Katalysator Recht und Technik gleichsam experimentell in einem Testparcours miteinander verbinden. Blockchain-basierte Wahlsysteme formen eine Kette nachvollziehbarer Elemente, die von der Stimmabgabe bis hin zur Stimmauszählung reicht. Dadurch lässt sich lückenlos nachverfolgen, dass jede Stimme auch in das Wahlergebnis einfließt. Das schließt (anders als im analogen Wahlverfahren) verloren gegangene Stimmen und Zählfehler praktisch aus. Die Struktur garantiert nicht nur eine lückenlose Nachvollziehbarkeit. Geeignete technische Maßnahmen – insbesondere kryptographische Verschlüsselungen – sichern zugleich die notwendige Geheimhaltung, ohne dass die Verifizierbarkeit darunter leidet. Damit bannen sie zugleich das Risiko, dass Dritte einzelne Stimmabgaben nachverfolgen. Ist die Blockchain einmal funktionsfähig aufgesetzt, schützt ihre innere und äußere Architektur grundsätzlich vor Manipulationen.

Explorer lassen sich als Wachposten einsetzen, die in das gesamte Wahlverfahren Einblick geben. Beobachter können in mehreren digitalen Räumen zugleich ihre Kontrollfunktion wahrnehmen. Entgegen einer verbreiteten Befürchtung bedarf es hierfür auch keiner spezifischen rechtlichen und technischen Fachkenntnisse. Die technisch teils hochkomplexen Mechanismen, die die Blockchain in sich vereinigt, sind durch passende Tools nutzerfreundlich und bequem durchsuchbar. Mathematische Verfahren liefern den Beweis für die Richtigkeit des Verfahrens. Tauchen doch Ungereimtheiten auf, lassen sie sich in der Blockchain-Struktur nachverfolgen. Denn verloren gegangene Stimmen, Zählfehler und ähnliche Unstimmigkeiten zertrennen die Stimmkette sofort. Irrläufer lassen sich daher an Ort und Stelle aufspüren. Ein solches digitales Wahlverfahren steht und fällt nicht damit, ob die Öffentlichkeit die eingesetzte Technik im Detail versteht. Es genügt die öffentliche Überprüfbarkeit.

Im Schatten dieser Stärken bleiben aber Risiken: Insbesondere Angriffe auf die Endgeräte des Nutzers sowie künftige Möglichkeiten, im Gefolge der Quantentechnologie-Entwicklung Verschlüsselung aufzubrechen und damit Stimmabgaben nachvollziehbar zu machen. Ob die Symbiose zwischen Recht und Technik tatsächlich gelingt, muss sich erst in der konkreten praktischen Umsetzung noch erweisen. Personalratswahlen eignen sich insofern in besonderer Weise als Laboratorium. Experimentierklauseln ebnen dafür den Weg. Sie bieten gleichsam einen Versuchsraum, in dem sich Risiken unter kontrollierten Bedingungen beobachten lassen. Gelingt das Experiment digitaler Wahlen, erbringt es nicht nur den Beweis der technischen Machbarkeit. Es entzieht einem generellen Misstrauen in digitale Wahlformate ein Stück weit den Boden und gewinnt im Idealfall jene für die demokratischen Verfahren zurück, die den Gang zur Urne längst gegen den Bildschirm getauscht haben. ■

162 Vgl. BSI, Technische Richtlinie TR-03162, Version 1.3.

163 BeckOK SozR/Bünnemann, 80. Ed. 2026, SGB IV § 54 Rn. 18, 20. Die konkrete Umsetzung in der Wahlordnung steht allerdings noch aus, BMAS, Änderung der Wahlordnung für die Sozialversicherung im Zusammenhang mit Online-Wahlen bei den Sozialversicherungswahlen, https://www.bmas.de/DE/Service/Gesetze-und-Gesetzesvorhaben/aenderung-der-wahlordnung-fuer-die-sozialversicherung.html. Die Wahlordnung verweist auf BSI, Technische Richtlinie TR-03169, Version 1.1.