

SAFEGUARDS AGAINST ELECTORAL FRAUD VS. ACCESSIBILITY AND CITIZENS' CONVENIENCE – NEED FOR CHANGES IN THE GERMAN ELECTORAL SYSTEM

Evelyn Armbruster¹ and Arne Pautsch²

DOI: 10.24989/ocg.v335.5

Abstract

Democratic elections are the basis of democracy. Allegations of electoral fraud lead to protests and violent clashes all over the world. In order to avoid such scenes, the electoral system has to be reliable and transparent. At the same time, voter turnout must be kept high in order to maintain the will of the people in a representative way. However, the required accessibility and citizens' convenience often seems to be in conflict with system security. Higher safeguards often comes with more formalisation and therefore less flexibility for the individual. This article shows how the German electoral system can be improved, while combining safety standards with citizens' convenience. For this purpose, significant weaknesses of voting in polling stations, postal vote, the count of votes and digitalization, especially e-voting are identified. To remedy these weaknesses, solutions from various European democracies are presented as reform approaches for the German electoral system.

Keywords: *electoral fraud, e-voting, postal vote, voting in polling stations, count of votes*

1. Introduction

The coincidence of various national and international developments is relevant to the security and citizens' convenience of the German electoral system. *First:* Elections and democracy lead to conflicts worldwide. Examples from 2018 are the elections in Turkey [13], Zimbabwe [21] and Russia [22]. A secure and transparent election system can avoid such incidents. *Second:* Globalization has changed the lifestyle of German citizens [30]. There are more and more Germans who have several residences or live abroad [18]. The German suffrage is based on the age, the nationality and the main residence of the citizens [38]. Therefore, globalization leads to greater complexity in suffrage. *Third:* Since the 1970s there has been a trend to declining voter turnout in political elections in Germany [40]. At the same time, the number of postal voters has been rising steadily [25]. *Fourth:* There is a tendency to make narrow majority results. Therefore, even the manipulation of a few votes can decide on political majorities [28]. *Fifth:* Accessibility and citizens' convenience are increasingly becoming the focus of public action. Long after taking over administrative tasks in economy, modern information and communication technologies are also

¹ Hochschule für öffentliche Verwaltung und Finanzen Ludwigsburg, Reuteallee 36, D-71634 Ludwigsburg

² Hochschule für öffentliche Verwaltung und Finanzen Ludwigsburg, Reuteallee 36, D-71634 Ludwigsburg

established by the government. So it is questionable whether the execution of integer election has to be restricted to a ballpoint pen and paper ballot [27].

2. Voting in polling stations

Voting at polling stations is generally considered to be particularly safe [3]. Although there is a trend towards an increasing use of postal voting, most German voters still vote in person at polling stations [16]. For this reason, manipulations could have far-reaching consequences, as the majority of votes cast could potentially be affected. This gives rise to the investigation of two areas of risk. On the one hand, the identification of identity in the polling station, on the other hand, problems in connection with electoral rolls.

2.1. Identity and polling station

The current practice in German polling stations is as follows: Before the ballot paper is thrown into the ballot box, the voter's identity is established by the electoral committee. To do this, it is sufficient to present the electoral notification and to establish the right to vote in the electoral roll. The presentation of an official photo ID is generally not required. It is mandatory only, if there are doubts to the identity of the voter or if the voter doesn't carry his electoral notification [38].

Although the current practice of identity check meets the spirit of citizens' convenience, the lack of a clear identification of each voter leads to a security gap in the German electoral system. The following scenario points out the importance of unambiguous identification:

Citizen *C* gives away/sells his election notification to the election fraudster *F* or *F* steals the electoral notification of *C*. In addition, *C* and *F* are assigned to *different polling stations*. *F* can therefore cast one vote at each of two different polling stations - his own polling station and in the polling station of *C*.

Case modification:

C and *F* are assigned to *the same polling station* of a major city. *F* first votes with its electoral notification. Dressed differently, *F* returns some time later to the same polling station to vote again with *C*'s election notification.

The case modification points to the changed social framework conditions due to the advancing urbanization. It is becoming more difficult for the electoral committee to reliably determine the identity of voters on the basis of the electoral notification [31]. A key recommendation in White and Johnston's report on electoral fraud in the UK is the introduction of an identity obligation at the polling station [41]. This approach can easily be transferred to the German system, as every German who has reached the age of 16 is required to have an identity card [32]. Other official photo IDs such as a driver's license or passport also appear to be suitable [41].

The use of biometric identification procedures for voter authentication in polling stations also represents a considerable reform approach. Biometric recognition methods identify a person based on unique behavioral and physical characteristics such as fingerprints, handprints, DNA, iris, voice or handwriting. Unlike other forms of proof of identity, biometric characteristics cannot be forgotten, lost, copied or stolen. The simultaneous improvement of security and citizens' convenience as well as the acceleration of the process are considered as advantages of biometric recognition procedures. Thus, voters would not have to carry an additional ID document with them

when using this form of authentication. On the other hand, there is the risk that physical characteristics are not replaceable. If the digital reproductions fall into the wrong hands, extensive misuse can occur [1].

2.2. Problems with electoral rolls

The electoral roll lists all persons who are eligible to vote in a local authority on Election Day [17]. The accuracy of the electoral register is of decisive importance for the conduct of a tamper-proof election. As an important control instrument, it should guarantee that only eligible persons are entitled to vote and that every voter is entitled to vote exactly once. All persons registered in the electoral roll receive an electoral notification [26]. In Germany, the electoral roll is drawn up *ex officio* [10]. For this purpose, the local authorities compile a separate electoral register for each general electoral district. The local population register serves as the basis [2].

By far the most serious loss of integrity in a voter register is the fact that a voter is listed in several registers at the same time [38]. This happens particularly due to data transmission errors between local authorities as a result of relocations. Duplicate entries may already be based on errors in local population registers [9]. Or may occur after the electoral roll has been drawn up. In this case, the voter receives several electoral notifications from different local authorities. The affected persons are thus actively informed of the possibility of double voting. In combination with a large number of incorrect data sets (around 4.8 million incorrect population registration data, as of 2008), there is a major security risk [39].

The introduction of a central population register for Germany and the introduction of a nationwide electoral register could remedy this problem. A central register would store all registration data of citizens at a central place (e.g. as in Austria at the Federal Ministry of the Interior) [24]. As a result of centralization, incorrect entries in several population registers would in fact be not possible. As explained, the electoral register is based on local registration data. Thus, the accuracy of the registration data takes a key role for the accuracy of the electoral roll.

A nationwide electronic electoral register would also be a solution to be considered. A nationwide electronic electoral roll is a register that centrally registers all German citizens entitled to vote. Combined with the use of networked voting computers, the link to the polling station of the home constituency could also be broken. Voters could then vote at any polling station in Germany. Adapting the ballot to current mobility behavior would also have a positive effect on the goal of citizens' convenience and accessibility. Furthermore, the lowering of the percentage of postal votes and non-voters is seen as a possible opportunity [2]. The problem of double registrations would also be superfluous, as there would only be one electoral register.

3. Postal vote

At present, postal voting is the only way of voting that is independent of time and place, and for this reason the most user-friendly form of voting [2]. It is possible for all eligible voters without stating reasons and is increasingly popular among citizens [8]. As a result of this development, postal votes can have an increasing influence on the outcome of elections. At the same time, postal voting involves numerous risks in bridging distances. This makes fraud in postal voting much easier than voting at the polling station [35].

3.1. Identity and postal voting

When applying for postal ballot documents, the following points are insufficient for a reliable identity verification:

- The information requested in the ballot paper proposal (surname, first name, date of birth, address) represents only a minor hurdle for abusive requests by third parties. In addition, the accuracy of a power of attorney can hardly be established by the local authority [38].
- Furthermore, § 27 Paragraph 1 BWO assesses the filing of an application by simple e-mail as equivalent to written form. As a result, e-mail applications without a qualified electronic signature are accepted. This passage is in competition with § 3 a Paragraph 2 VwVfG according to which only e-mails with a qualified electronic signature are equivalent to written form [28]. Concerns about this procedure are the easy falsification of e-mails and the simplicity of creating e-mail addresses with the data of a voter [4].
- The ballot paper may be sent to an address other than the address of residence or delivered to a third party. This increases the citizens' convenience but also the susceptibility to manipulation [38]. The control notification sent at the same time to the residential address [11] increases the protection against manipulations only relatively because this only informs the citizen concerned. The delivery of the election documents by a simple letter to the address of a perhaps unauthorized person takes place anyway.

In order to counter the shortcomings described above, the formulation of Austrian electoral law offers a suitable alternative: In Austria it is generally necessary to establish the applicant's identity. For oral and written applications, the voter must prove his or her identity, for example by presenting an official photo ID or passport number. However, there are two exceptions for written applications. On the one hand, applicants known to the authorities do not have to prove their identity. On the other hand, the qualified electronic signature acts as proof of identity when an application is submitted by e-mail. The postal voting documents requested without a qualified electronic signature are sent by registered letter and must be received in person. Election documents requested with a qualified electronic signature end up in the applicant's letterbox as a standard letter [23].

3.2. Problems with postal delivery

The postal vote requires the transmission of the ballot letter from the private sphere of the voter to the ballot box. For this reason, it seems advisable to take a closer look at the weaknesses in the transmission medium - the postal system [3]. In Germany there is no legal provision for the secure delivery of postal voting documents. At present, postal voting documents are sent to voters by a simple letter [28]. The eligible voter bears the risk of loss or delays by post [38]. The confidentiality and integrity of postal votes may be violated by postal employees. Possible worst case scenarios are opening and reading the contents of the election letters - vote and voter identity - as well as changing, throwing away or adding new election letters [3].

A possible reform approach to counter problems with the sending of postal voting documents is the legal establishment of a secure form of delivery. Here, too, it is worth taking a look at Austrian electoral law: § 5a Paragraph 8 BPräsWG defines various forms of delivery. As mentioned above, postal voting documents are generally sent by registered letter. A simple letter is sufficient if the application has been received in person or by e-mail with a qualified electronic signature.

Furthermore, the particular risk of manipulation in medical and nursing homes is taken into account - in the case of nursing home residents, the registered letter must be addressed exclusively to them and marked like this: "Not to authorized postal representatives" [6].

In order to increase security when returning election letters, official notes on receipt should be considered as a reform approach. At present, only election letters that are received late get such a note [11]. The purpose of the entry note is: Upon request, the voter can obtain information from the local authority whether his election letter reached the local authority on time. In order to make this information possible, it would be necessary to compare the ballot paper number printed on the ballot paper with the ballot paper list [38]. Finally, both or a combination of both reform approaches have the potential to increase security in the delivery and return of postal voting documents without resulting in a loss of civic convenience. Under the premise that "care and accuracy have the highest priority over thrift" [38]³, concerns about administrative and cost issues can be invalidated.

4. Counting

The election must not only be protected against attacks from third parties, but equally important is protection against election fraud from the inside - namely by the state organizing the election. The points of attack addressed refer to the counting of votes and the storage of postal votes. Intentional manipulation of the results presupposes agreement in the election committee in the absence of election observers at the same time. Under these conditions, the following manipulations are conceivable: The incorrect intentional assignment of votes to another party or the invalidation of votes although these would be considered valid. Moreover, the officials responsible for safe keeping the postal votes could exchange the election envelopes or add new ones. As long as the number of envelopes added remains smaller than the number of registered postal voters, the risk of discovery is expected to be low [35].

The described attacks would not cause any irregularities in the checksums of German election reports. With the focus on the risk of the election committee adding ballot papers, the content of the election report is insufficient and therefore in need of reform. At present, the election report does not contain any information on the number of ballots received, used, unused or damaged [29]. Rather, "the local authority [...] hands over official ballot papers in sufficient numbers to the head of each electoral district before the start of the electoral process" [11].⁴ The inclusion of these fields could increase transparency and thus meet possible distrust towards the electoral committee [29].

Furthermore, the use of technical means (e-counting) could offer a new perspective for integer counting. In this way, incorrect interpretations of ballots or unintentional counting errors could be avoided [7]. E-counting systems have been used in Switzerland's government practice since 2001. The Chaos Computer Club has criticized the use of these systems [12]. This raises concerns about a real quality improvement. In addition, the use of electronic voting devices in Germany is limited by the Constitutional Court's ruling on voting computers [7].

5. E-Voting

The most important voting channel for electronic voting today is online voting. Voting online is similar to postal voting, a convenient form of voting for citizens. Like any other voting channel, e-

³ please refer Schreiber, § 36 Rn. 5 e. (My translation, my emphasis)

⁴ please refer Bundeswahlordnung, § 49 Nummer 3. (My translation, my emphasis)

voting must comply with the principles of democratic elections [15]. A particular challenge for information technology is the implementation of the electoral principles of the public and secrecy of the election.

The decision of the German Constitutional Court in 2009 on the use of voting computers in parliamentary elections is of great importance for the principle of public. According to the principle of public, the central steps of electoral action and result determination must be verifiable. Due to violation of this electoral principle while using voting computers in German parliamentary elections, the law on the use of voting equipment was declared unconstitutional. Nevertheless, the ruling of the Constitutional Court does not exclude the use of electronic voting machines [7]. This fundamental decision on public voting is also of great influence beyond the borders: At the European level, the Committee of Ministers created the Recommendation CMRec(2017)5 on the standards of e-voting. This Recommendation establishes verifiability requirements that take into account the view of the public principle according to German case law.

In its Recommendation, the Council of Europe proposes review mechanisms in the sense of end-to-end verifiability for the implementation of the principle of the public [14]. The end-to-end verifiability is a security mechanism through which the voter can follow the complete path of his vote (casting of vote - transfer of vote - storage of vote - counting of votes) [3]. In the same way, the anonymization of voter identity by means of information technology is of eminent importance for the protection of electoral secrecy. Accordingly, the e-voting procedure - in particular the counting - must be designed in such a way that no connection between the unencrypted vote and the voter can be reconstructed [15]. In order to meet this requirement, anonymization must take place before the vote is cast. Nevertheless, technical security measures are not sufficient for system security. Secure e-voting systems can only be created through the interaction of technical and organizational safeguards [33]. However, a remaining risk for system security can never be ruled out [38]. Whether this remaining risk is acceptable is a political question [34].

A particular problem for the reintroduction of e-voting in Germany is the rare use of the electronic functions of the identity card. The online ID card function (eID function) of the Identity card allows citizens to identify themselves safely on the Internet [5]. The reliable identification of voters on the Internet is a basic requirement for online elections. In the absence of a reliable identification on the Internet, online voting would not have been an option for two-thirds of Germans eligible to vote in 2015 [20]. This limits the potential of e-voting enormously.

5.1. Evaluation in the context of postal voting

As described for postal voting, bridging distances involves numerous risks. Online voting and postal voting are both forms of remote voting. Finally, it has to be assessed whether online voting could be an alternative to postal voting for the German electoral system. For evaluation, the most critical electoral law principles for distance voting will be used: The protection of electoral secrecy and the guarantee of principle of public.

As with postal voting, the voter is responsible for a secret, personal and uninfluenced vote in online voting. Both forms of voting are outside the control of the electoral committee and the public [3]. Online voting could offer new opportunities for protecting electoral secrecy. For example, the Estonian online voting software allows voters to overwrite their votes as often as they like until the end of the voting period. Only the last vote is included in the election result [19]. This seems a suitable measure to counter undue influence, as the voter can change the vote content at any time.

Furthermore, the online election could offer a new perspective for the public principle. In postal voting, the voter is currently unable to understand what happens to his or her vote after sending the ballot letter. This is not the case with online voting: individual verifiability allows voters to verify that their votes have been entered correctly in the ballot box [3]. The universal verifiability enables interested persons to observe the correct counting from their home computer without being restricted to a single polling station [36].

The end-to-end verifiability makes the entire voting process reproducible and enables complete error tracking. Independent of the cryptographic methods used, the greatest information technology skill lies in transferring this mathematical-cryptographic evidences into a form that is comprehensible to the citizen [37]. In spite of the strengths shown, it remains to be taken into account: A careful evaluation of existing threats in online elections is essential and at the same time extremely difficult. Manipulations could expand largely in online elections. In postal voting, this risk is considerably limited by the decentralized structure of the postal voting districts [3].

6. Conclusion

The agreement of both objectives, protection against manipulation on the one hand and citizen convenience on the other, is of central importance for the quality of an electoral system. Protection against possible fraud makes an important contribution to the legitimation of political decisions. It ensures that citizens have the necessary confidence in democracy. An equally important part is the system's civic convenience. With the key words comfort, accessibility and comprehensibility, the component of citizen convenience ensures a high participation rate.

As the article shows, improving protection against possible manipulation contradict the objective of citizen convenience in many fields. Conversely, improvements in citizen convenience often lead to lower security against manipulation. In order to combine these often competing aims, it is necessary to make an appropriate assessment in each field. Only in this way a suitable balance can be found for the entire system.

7. References

- [1] AWAD, M. / LEISS, E., No ballot left behind: Using biometric identification to facilitate voter authentication in: Globale Sicherheit und proaktiver Staat – Die Rolle der Rechtsinformatik, Tagungsband des 13. Internationalen Rechtsinformatik Symposions (IRIS), 2010, p. 77 – 83.
- [2] BERTELSMANN STIFTUNG, „Zeitgemäß Wählen“ – 8-Punkte-Plan zur Steigerung der Wahlbeteiligung in: Einwurf Zukunft der Demokratie Sonderausgabe 1-2, 2016, https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/ZD_EINWURF_Sonderausgabe_1-2_2016.pdf, [28.05.2018].
- [3] BRÄUNLICH, K. / GRIMM, R., Einfluss von Wahlszenario auf Geheimheit, Privatheit und Öffentlichkeit der Wahl, 2016, https://kola.opus.hbz-rw.de/opus45kola/frontdoor/deliver/index/docId/1316/file/Einfluss_von_Wahlszenario_auf_Geheimheit_Privatheit_und_Oeffentlichkeit_der_Wahl.pdf, [01.05.2018].
- [4] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK, Gefährliche Kuckuckseier: E-Mails mit falschem Absender, 2017, abrufbar im Internet: [https://www. bsi-](https://www.bsi-)

fuer-buerger.de/BSIFB/DE/Risiken/SpamPhishingCo/GefaeltschteAbsenderadressen/gefaelschteabsenderadressen_node.html, [21.07.2018].

- [5] BUNDESMINISTERIUM DES INNEREN FÜR BAU UND HEIMAT, Die elektronischen Funktionen des Personalausweises, https://www.personalausweisportal.de/DE/Buergerinnen-und-Buerger/Der-Personalausweis/Funktionen/funktionen_node.html, [11.08.2018].
- [6] BUNDESPRÄSIDENTENWAHLGESETZ 1971 ÖSTERREICH, In der Fassung der Bekanntmachung vom 25.02.1971.
- [7] GERMAN CONSTITUTIONAL COURT - 2 BvC 3/07, 2 BvC 4/07, Urteil des Zweiten Senats vom 3. März 2009, Fundstelle 123, 39 – 88, https://www.bundesverfassungsgericht.de/Shared_Docs/Downloads/DE/2009/03/cs20090303_2bvc000307.pdf?__blob=publicationFile&v=1, [05.03.2018].
- [8] GERMAN CONSTITUTIONAL COURT - 2 BVC 7/10, Beschluss vom 09. Juli 2013, Fundstelle 134, 25 – 32, https://www.bundesverfassungsgericht.de/SharedDocs/Downloads/DE/2013/07/cs20130709_2bvc000710.pdf?__blob=publicationFile&v=1, [20.07.2018].
- [9] BUNDESMELDEGESETZ, In Fassung der Bekanntmachung vom 3. Mai 2013, zuletzt geändert durch Artikel 11 Absatz 4 des Gesetzes vom 18. Juli 2017.
- [10] BUNDESWAHLGESETZ, In der Fassung der Bekanntmachung vom 23. Juli 1993, zuletzt geändert durch Artikel 2 Gesetzes vom 10. Juli 2018.
- [11] BUNDESWAHLORDNUNG, In der Fassung der Bekanntmachung vom 19. April 2002, zuletzt geändert durch Artikel 5 des Gesetzes vom 8. Juli 2017.
- [12] BURTSCHER, M., Parlament übt Kritik an elektronischer Auszählung von Stimmzetteln in: St. Galler Tagblatt vom 07.06.2018, <https://www.tagblatt.ch/schweiz/kritik-an-elektronisch-er-auszahlung-ld.1027109>, [01.08.2018].
- [13] BUTTKEREIT, C., Analyse der Türkei-Wahl –Mehr Macht, aber auch mehr Opposition in: Tagesschau.de vom 25.06.2018, https://www.tagesschau.de/ausland/erdogan-wahlsieg-107~_origin-f669dc2b-d3d2-46be-b517-9c3db6b66ae3.html, [10.08.2018].
- [14] COUNCIL OF EUROPE, Explanatory Memorandum to Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting, vom 14.06.2017, https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=090000168071bc84, [15.05.2018].
- [15] COUNCIL OF EUROPE, Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting, vom 14.07.2017, <https://rm.coe.int/CoERMPublicComonSearchServices/DisplayDCTMContent?documentId=0900001680726f6f>, [15.05.2018].
- [16] DER BUNDESWAHLLEITER, Anteil der Briefwählerinnen und Briefwähler bei den Bundestagswahlen 1994 – 2017 nach Ländern, 2017, https://www.bundeswahlleiter.de/dam/jcr/b4aeabb8-7fac-473e-8581-cd718cb7a007/BTW_ab94_briefwahl.pdf, [01.06.2018].

-
- [17] DER BUNDESWAHLLEITER, Wählerverzeichnis und Umzug, 2017, <https://www.bundeswahlleiter.de/bundestagswahlen/2017/informationen-waehler/waehlerverzeichnis-umzug.html>, [01.06.2018].
- [18] DER TAGESSPIEGEL, Zweitwohnungsboom verändert Städte, vom 29.05.2017, <https://www.tagesspiegel.de/wirtschaft/multilokalitaet-zweitwohnungsboom-veraendert-staedte/19863200.html>, [15.03.2018].
- [19] DEUTSCHER BUNDESTAG, Online-Wahlen Erfahrungen in anderen Staaten und (verfassungs-)rechtliche Voraussetzungen für eine Einführung in Deutschland, 2014, <https://www.bundestag.de/blob/412066/df70d4a9753c21463cff4030d510cf06/wd-3-030-14-pdf-data.pdf>, [28.04.2018].
- [20] DIE WELT, Deutschland verschläft die Ausweis-Revolution, vom 10.06.2015, <https://www.welt.de/wirtschaft/article142233969/Deutschland-verschlaeft-die-Ausweis-Revolution.html>, [10.08.2018].
- [21] GENTH, J., Simbabwe nach der Wahl – Proteste eskalieren – mehrere Tote in: Tagesschau.de vom 01.08.2018, <https://www.tagesschau.de/ausland/simbabwe-wahl-107.html>, [10.08.2018].
- [22] HEBEL, C., Putin gewinnt Russland-Wahl – Ein Sieg wie gemacht in: Spiegel Online vom 18.03.2018, <http://www.spiegel.de/politik/ausland/russland-wahl-wie-sich-wladimir-putin-seinen-sieg-gemacht-hat-a-1198704.html>, [10.08.2018].
- [23] HELP.gv.at, Wahlkarte/Stimmkarte, 2018, abrufbar im Internet: <https://www.help.gv.at/Portal.Node/hlpd/public/content/32/Seite.320520.html>, [21.07.2018].
- [24] HELP.gv.at, Zentrales Melderegister (ZMR), 2018, <https://www.help.gv.at/Portal.Node/hlpd/public/content/99/Seite.991731.html>, [01.06.2018].
- [25] LANDESZENTRALE FÜR POLITISCHE BILDUNG BADEN-WÜRTTEMBERG, Wahlstatistik, 2017, http://www.bundestagswahl-bw.de/wahlstatistik_bw17.html, [26.12.2018].
- [26] LANDESZENTRALE FÜR POLITISCHE BILDUNG BADEN-WÜRTTEMBERG, Wie wird gewählt?, http://www.bundestagswahl-bw.de/stimmabgabe_btw2017.html, [01.06.2018].
- [27] LINDENAU, I., Rechtliche und tatsächliche Probleme der elektronischen Wahl, Leibniz-Universität Hannover, Masterarbeit, 2006/2007, https://www.eulisp.de/tl_files/eulisp%20abschlussarbeiten/jahrgang%20neuer/MA_Inga%20Lindenau_Elektronische%20Wahl.pdf, [02.05.2018].
- [28] MÜLLER-TÖRÖK, R. / PAUTSCH, A., Stochastische Verfälschung von Wahlergebnissen bei grenzüberschreitender Briefwahl? in: Verwaltung und Management, Heft 4, 2015, p. 192 – 197.

-
- [29] OSCE / ODIHR- WAHLBEWERTUNGSMISSION, Wahl zum Deutschen Bundestag am 27.09.2009 – Bericht, 2009, <https://www.osce.org/de/odihr/elections/germany/40879?download=true>, [20.01.2018].
- [30] PAUTSCH, A. / MÜLLER-TÖRÖK, R., Das Wahlrecht der Auslandsdeutschen nach § 12 Abs. 2 BWG auf dem neuerlichen Prüfstand? Eine Analyse aus juristischer und verwaltungswissenschaftlicher Sicht in: Zeitschrift für Parlamentsfragen (ZParl), Heft 4, 2016, p. 851 – 866.
- [31] PICKLES, E., Securing the ballot, 2016, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/545416/eric_pickles_report_electoral_fraud.pdf, [20.01.2018].
- [32] PERSONALAUSSWEISGESETZ, In der Fassung der Bekanntmachung vom 18. Juni 2009, zuletzt geändert durch Artikel 4 des Gesetzes vom 18. Juli 2017.
- [33] PROSSER, A., Transparency in eVoting: Lessons learnt in: Transforming Government: People, Process and Policy, Band 8, Ausgabe 2, 2014, p. 171 – 184.
- [34] REINERS, M., E-Voting in Estland: Vorbild für Deutschland?, 2017, <http://www.bpb.de/apuz/255967/e-voting-in-estland-vorbild-fuer-deutschland?p=all>, [02.08.2018].
- [35] RENZ, J., Gibt es Anzeichen von Wahlfälschung bei Bundestagswahlen?, 2018. abrufbar im Internet: https://www.ssoar.info/ssoar/bitstream/handle/document/55715/ssoar-2018-Renz-Gibt_es_Anzeichen_von_Wahlfalschung.pdf?sequence=3, [19.05.2018].
- [36] RICHTER, P. / HUPF, K. / GRIMM, R., Juristisch-Informatische Herleitung von Sicherheitsanforderungen für Internetwahlen am Beispiel des Grundsatzes der Öffentlichkeit der Wahl in: Globale Sicherheit und proaktiver Staat – Die Rolle der Rechtsinformatik, Tagungsband des 13. Internationalen Rechtsinformatik Symposions (IRIS), 2010, p. 95 – 102.
- [37] RICHTER, P. / LANGER, L. / U. A., Verifizierbarkeit und Öffentlichkeitsgrundsatz bei elektronischen Wahlen in: Globale Sicherheit und proaktiver Staat – Die Rolle der Rechtsinformatik, Tagungsband des 13. Internationalen Rechtsinformatik Symposions (IRIS), 2010, p. 61 – 66.
- [38] SCHREIBER, W., Kommentar zum Bundeswahlgesetz, Auflage 10, 2017.
- [39] SPIEGEL ONLINE: Schäuble plant zentrales Bundesmelderegister, vom 27.06.2008, <http://www.spiegel.de/politik/deutschland/einwohnerdaten-schaeuble-plant-zentrales-bundesmelde-register-a-562375.html>, [01.06.2018].
- [40] STATISA, Wahlbeteiligung bei den Bundestagswahlen in Deutschland von 1949 bis 2017, <https://de.statista.com/statistik/daten/studie/2274/umfrage/entwicklung-der-wahlbeteiligung-bei-bundestagswahlen-seit-1949/>, [13.04.2018].
- [41] WHITE, I./ JOHNSTON, N., Electoral fraud since 2010, 2017, <http://researchbriefings.files.parliament.uk/documents/SN06255/SN06255.pdf>, [20.01.2018].