DOI 10.5817/MUJLT2025-1-4

EVOTING AT THE GERMAN SOCIAL ELECTIONS – LESSONS LEARNT

by

DOMENICA BAGNATO * ROBERT MÜLLER-TÖRÖK †
ÁLEXANDER PROSSER ‡ ROBERT STEIN §

With an electorate of 52m the German Social Elections (Sozialwahl) is arguably one of the largest single elections in the European Union. It elects representatives of all people under social security and has been conducted through postal voting only for decades. In 2023 eVoting was introduced as an additional voting channel for the first time. This paper focuses specifically on the eVoting part, particularly the technical requirements and the voting protocol used. It analyses them against general voting principles and the relevant Recommendation of the Council of Europe.

KEY WORDS

eVoting, Social Elections, voting principles, envelope protocol, homomorphism, Council of Europe Recommendation.

1. GENERAL FRAMEWORK

The "Sozialwahl" or Social Election is the third-largest election in Germany, about 52m people with either mandatory social security or pensioners elect their representatives in the self-governing bodies of the social security institutions. The voting right is not restricted to German citizens above 18 years of age like in General Elections, but also granted to foreigners who work

* University of Economics and Business, Vienna, email: domenica.bagnato@wu.ac.at
† University of Public Administration and Finance, Ludwigsburg, email: robert.mueller-toeroek@hs-ludwigsburg.de
‡ University of Economics and Business, Vienna, email: alexander.prosser@wu.ac.at
§ Federal Ministry of the Interior, Vienna, email: robert.stein@bmi.gv.at. This paper expresses his private opinion.

and hence pay mandatory social security or are pensioners and the voting right is also granted to working people from 16 years of age on.[1]

These representatives are in the so-called "Social Parliaments", one each in every social security institution. These institutions are the public German Pension Insurance and five health insurance funds (five large out of a total of 95 health insurance funds existing in Germany in 2023).[2] Their actual power and influence is limited to advice and supervision, normally they do not interfere in daily politics and business.[3] So, as compared to General Elections or Elections to Federal State Parliaments, city councils or county councils, the election is of far less significance – despite being an official, nationwide election governed by the law with voter rolls and all the requisites of a "normal" election.

It is regulated in Social Code IV, §§ 43-66.[4] The Federal Minister of Labour and Social Affairs issues the Election Decree, which is rarely changed.[5] The Social Election itself does not attract much public attention, political parties do not stand for this election and it is rarely disputed in the courts, hence it is suitable for an eVoting pilot. Different to other countries and elections, the competent court of appeal for this election is either the Social Court at the location of the German Pension Insurance or of the respective health insurance fund whose election is disputed. So the judicial appeal is not centralized at one single court, but rather spread among up to six out of 68 regional Social Courts at the first level, one or more out of 14 Social Courts of Federal States at the second level and the Federal Social Court at the third level.[6] So a final decision could appear years after the election was originally contested.

---

1 Cf. Bundesregierung (2023) *Wissenswertes zur Sozialwahl 2023*. [online] Berlin. Available: https://www.bundesregierung.de/breg-de/aktuelles/sozialwahl-2023-2188062 [Accessed 20 July 2025]

2 GKV Spitzenverband. *Die gesetzlichen Krankenkassen*. [online] Bonn. Available from: https://www.gkv-spitzenverband.de/krankenversicherung/kv_grundprinzipien/alle_gesetzlichen_krankenkassen/alle_gesetzlichen_krankenkassen.jsp [Accessed 19 June 2025]

3 Ibid.

4 *Sozialgesetzbuch (SGB) Viertes Buch (IV) - Gemeinsame Vorschriften für die Sozialversicherung* - (Artikel I des Gesetzes vom 23. Dezember 1976, BGBl. I S. 3845) (Social Code IV). In German. Available from: https://www.gesetze-im-internet.de/sgb_4/ [Accessed 20 June 2025]

5 Bundesministerium für Arbeit und Sozialordnung (1997). *Wahlordnung für die Sozialversicherung* (Election Decree for the Social Elections). In German. Available from: https://www.gesetze-im-internet.de/svwo_1997/ [Accessed 20 June 2025]

6 Cf. Nakielski, H. (2022). *Gerichte und Richter:innen der Sozialgerichtsbarkeit*. [online]. Available from: https://netzwerk-sozialrecht.net/gerichte-und-richterinnen-der-sozialgerichtsbarkeit/ [Accessed 20 June 2025]

The Social Election was introduced in 1953 and has been postal voting only, ie. pure distance voting. This makes it, at least from a cost perspective, interesting for an eVoting pilot. The participation has been declining for decades; despite the eVoting pilot, participation in the Social Election reached an all time-low in 2023 with a turnout of 22.43 % (30.42 % in 2017, the last election before the COVID-19-Pandemic).[7]

In 2022, it was decided that eVoting shall be offered as an alternative voting channel at the Social Election 2023; hence, the law had to be adapted to enable eVoting. For the purposes of the eVoting pilot, §§ 194a - § 194d were added to the Social Code V[8], empowering the Federal Minister of Health to issue an Online Election Decree to enable this pilot. There are two main documents governing the eVoting part of the Social Election:[9]

- The Online Election Decree (in the following "Decree") by the Federal Ministry of Health[10]
- Federal Office for Information Security BSI (2023) Technical Guideline TR-03162[11]

These two documents should be seen as one, because § 194c (1) requires the Federal Minister of Health to reconcile with BSI, while § 194c (2) required the office to produce the Technical Guideline. Right at the beginning of the Decree in § 1, it is made clear that this eVoting election, even though not a political election, serves as a "model project" for further application

[7] Der Bundeswahlbeauftragte für die Sozialversicherungswahlen (2024). *Schlussbericht des Bundeswahlbeauftragten für die Sozialversicherungswahlen zu den Sozialwahlen 2023*. Final Report of the Federal Election Commissioner for the Social Election. Berlin: Bundesministerium für Arbeit und Soziales. Available from: https://www.bmas.de/SharedDocs/Downloads/DE/Meldungen/2024/bundessozialwahl-2023-schlussbericht.pdf?__blob=publicationFile&v=1 [Accessed 20 June 2025]

[8] *Sozialgesetzbuch (SGB) Fünftes Buch (V) - Gesetzliche Krankenversicherung* - (Artikel 1 des Gesetzes v. 20. Dezember 1988, BGBl. I S. 2477) (Social Code V). In German. Available from: https://www.gesetze-im-internet.de/sgb_5/ [Accessed 20 June 2025]

[9] Note that the provisons of the Social Code are relatively abstract, the details are, not unusual in German legislation, regulated by a decree of a Federal Minister.

[10] Federal Ministry of Health (2020). *Verordnung über die technischen und organisatorischen Vorgaben für die Durchführung einer Online-Wahl im Rahmen des Modellprojekts nach § 194a des Fünften Buches Sozialgesetzbuch*. Berlin. In German. Available from: https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/3_Downloads/Gesetze_und_Verordnungen/GuV/O/Online-Wahl-VO_Bgbl.pdf [Accessed 20 June 2025]

[11] Bundesamt für Sicherheit in der Informationstechnik (2023). *Technische Richtlinie TR-03162, Version 1.3, 3.2.2023*. Bonn. In German. Available from: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03162/TR-03162_node.html#:~:text=Die\%20Technische\%20Richtlinie\%20TR\%20\%2D03162,Briefwahl\%20auch\%20Online\%2DWahlen\%20anzubieten [Accessed 20 June 2025]

– as § 194a already stated before. Hence, there is an increased interest in how this eVoting was implemented; it also implies that Council of Europe Recommendation CM/Rec(2017)5[12], which only applies to political elections, indirectly does apply and should hence be adhered to.

The Decree further stipulates that the participating social insurance institutions commission a service provider to run the online election system. The guidelines to follow are the

- BSI Basic IT Protection standard, "IT-Grundschutz"[13] and
- Technical Guideline TR-03162, which, at the time the Decree was passed, was still in its draft status.

In § 8, the Decree requires an independent security validation by an external expert, however only in view of the Basic IT Protection, not the protection of general voting principles.[14] Therefore, the external expert validation was to check for instance, whether backups were made and general IT security was maintained, but did not cover for instance protection of voting secrecy or any other specifics of eVoting. This is an interesting approach to eVoting security. § 194a (4) of the Social Code V stipulates that the voting principles listed in § 45 (2) of the Social Code IV shall be followed "with a view to the technical features also in the online elections"[15] The principles listed in this paragraph include only three, namely

- Free suffrage
- Secret suffrage
- Accountability in the terminology of the CoE, here in the German terminology (Public) Auditability of the whole election[16]

[12] Council of Europe 2017. *Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting*, Strasbourg. Available from: `https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=0900001680726f6f` [Accessed 28 March 2025]

[13] Federal Office for Information Security (2018). *Guide to Basic Protection based on IT-Grundschutz*. Bonn. In German. Available from: `https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/Basic_Security.html?nn=908032` [Accessed 20 June 2025]

[14] Cf. reference in § 8 to § 3 Paragraph 4 Sentence 1. This reference hence only covers the basic protection (IT-Grundschutz in the terminology used in Germany).

[15] Cf. Sozialgesetzbuch (SGB) Fünftes Buch (V) - Gesetzliche Krankenversicherung (Social Code V), *Op. cit.*, § 194a, our translation

[16] This term "Grundsatz der Öffentlichkeit der Wahl" means that the whole election process, except for casting the ballot, occurs in public and is fully auditable. In German practice this also includes each citizen's right to watch the emptying of the ballot boxes and the counting in person.

It has to be added that TR-03162 Section 2.1.1.3 requires a risk analysis for various specific attacks against the voting system, such as "ballot stuffing" or an "Italian attack" (meaning compromising voting secrecy[17]), however, this is not subject to the external security validation according to § 8 of the Decree and nowhere and in no shape or form does TR-03162 refer to CM/Rec(2017)5, which would actually have been a natural reference point for eVoting in a Member State of the Council of Europe. The Recommendation would have also provided an easy-to-use reference point with pre-defined requirements and attack vectors. Such reference would have also been perfectly in line with the "model character" of the project for political elections.

2. THE GENERAL VOTING PROTOCOL

The main eVoting protocol follows an Enveloping approach, with explicit reference to the system used in Estonia as depicted in Figure 1[18].

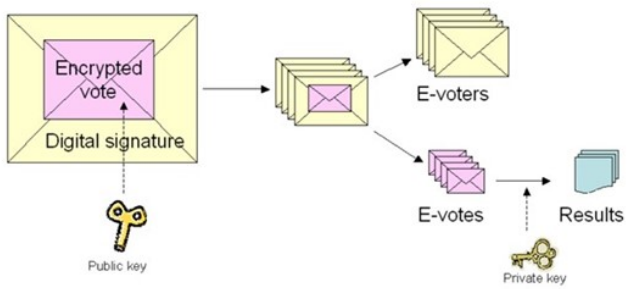

Figure 1: General envelope protocol

Here a brief description and analysis of the "pure" envelope protocol as used in Estonia.

[17] Whereby the literature mainly seems to focus on voter coercion (Italian coercion attack), see for instance Huber, N. et al. (2022). Kryvos: Publicly Tally-Hiding Verifiable E-Voting. In: Yin, H. and Stavrou, A. (eds.) *CCS 2022: Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, Los Angeles, 7 Nov. USA: Association for Computing Machinery. Available from: https://doi.org/10.1145/3548606.3560701 [Accessed 20 June 2025], pp. 1443–1457 and Peng, K. and Bao, F. (2009). A Design of Secure Preferential E-Voting. In: Ryan, P.Y.A. and Schoenmakers, B. (eds.) *Vote-ID 2009: International Conference on E-Voting and Identity*, Luxembourg, 7-8 September. Germany: LNCS 5767. Available from: https://link.springer.com/chapter/10.1007/978-3-642-04135-8_9 [Accessed 20 June 2025], pp. 141-156

[18] Estonian National Electoral Committee (2010). *E-Voting System, General Overview*, Tallinn. Available from: https://www.valimised.ee/sites/default/files/uploads/eng/General_Description_E-Voting_2010.pdf [Accessed 20 June 2025], p. 10, Figure 1

The protocol assumes (i) an asymmetric, for instance RSA[19], key pair (external E, domestic D) of which E is delivered to the eVoter by the voting application and (ii) a digital signature available to the voter. The voter fills in the ballot (or casts a blank vote), whereupon it is encrypted with public key E giving E(ballot), the "inner envelope". Private key D is only known to the election committee and may also be distributed among the members of the committee.[20] The voter adds his or her signature to the now encrypted ballot ("outer envelope"). This combined envelope structure is sent to the electronic ballot box. The ballot box thereby contains the information who voted for whom only protected by the encryption of the inner envelope. In the tally, the signatures on the outer envelope are verified and the usual checks performed (eligible voter, only one vote cast, no vote cast by alternative channels, etc.). The outer envelope is then "removed", and the inner envelope forwarded to the election committee, who apply their private key D to open (decrypt) the ballot, which is then counted (cf. Figure 1 for the process).

This protocol at first glance corresponds to the standard postal voting procedure of two envelopes, their separation and the insertion of the inner ballot envelope in the ballot box. It therefore holds an intrinsic appeal to election officials who recognise their postal voting standard procedure. However, Enveloping has some serious and well-documented flaws:

a. The paper analogy does not hold. If a paper ballot envelope is taken out of the outer postal envelope, it is physically not there anymore as the paper envelope exists just once. Mixed with other ballot envelopes, voting secrecy can easily be achieved. In the electronic media, however, this analogy does not hold. The data records of (digital voter signature, E(ballot)) exist, whether in mirrored storage media, backups or illicit copies. Once the election committee private key D is known, it can easily be applied to give D(E(ballot)) = ballot, which in turn enables to reconstruct (digital voter signature, ballot) and hence the mass violation of voter secrecy. In that, Enveloping, as used for Estonian eVoting, violates the following standards of CM/Rec(2017)5:

[19] Rivest, R. L., Shamir, A., and Adleman, L. (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM, 21(2)*, Available from: `https://dl.acm.org/doi/pdf/10.1145/359340.359342` [Accessed 20 June 2025], pp. 120-126

[20] Prosser, A. (2004) Implementation of Quorum-Based Decisions in an Election Committee. In: Traunmüller, R. (ed.) *DEXA/EGOV 2004: 15th International Workshop on Database and Expert Systems Applications*, Zaragossa, 30 August – 3 September. Germany: LNCS 3183, pp. 122-127

- E-voting shall be organised in such a way as to ensure that the secrecy of the vote is respected at all stages of the voting procedure. (Standard 19).
- The e-voting process, in particular the counting stage, shall be organised in such a way that it is not possible to reconstruct a link between the unsealed vote and the voter. Votes are, and remain, anonymous (Standard 26).
As seen above, it is possible to construct a link between the unsealed vote and the voter once the electronic ballot box and the private key of the election committee are brought together.
Where applicable, also Standard 25 is violated simply by analogy: *E-voting shall ensure that the secrecy of previous choices recorded and erased by the voter before issuing his or her final vote is respected*.

b. The ballot box data constitutes an inherent risk and hence should be destroyed as soon as possible. This however makes a judicial review of the eVoting virtually impossible as there are no artefacts left. An example may be the Austrian student elections in 2009, where the voting data was deleted prematurely and contrary to the applicable decree, which rendered the judicial review by the Austrian Constitutional Court rather difficult.[21]

c. This property also makes an independent recount virtually impossible (or meaningless). Either the mere ballots are handed over to the recount, which makes the recount completely dependent on the integrity of the election administration it is supposed to check; or ballot box and private key D are handed over giving the election committee at least the technical ability to verify how each voter voted. This, however, violates at least Standard 18: *The system shall provide sound evidence that only eligible voters' votes have been included in the respective final result. The evidence should be verifiable by means that are independent from the e-voting system*. Since there is no independent recount, the independent verification of the result is not possible.

For a detailed discussion of Enveloping in general and its deficiencies we refer to the literature.[22] More details on the process itself were published by

[21] Balthasar, A. and Prosser, A. (2012). E-Voting in der Sonstigen Selbstverwaltung - Anmerkungen zu VfGH vom 30. Juni 2011, B 1149, und vom 13. Dezember 2011, V 85-96. *Journal für Rechtspolitik (JRP)*, 2012(1), pp. 47-86.

[22] Springall, D. et al. (2014). Security Analysis of the Estonian Internet Voting System. In: *CCS'14: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communication*

State Electoral Office of Estonia.[23] The system used at the social elections, however, had two substantial deviations from the Estonian algorithmic original discussed in the two following sections.

3. EXTENSION 1: HOMOMORPHIC ENCRYPTION

One may conclude that also TR-03162 does not fully believe that Enveloping is a sufficient safeguard against compromising as it enables ("can be used") a homomorphic encryption of the votes (Section 4.5.2 of Technical Guideline TR-03162). Generally, homomorphic encryption enables mathematical operations on encrypted data without access to the unencrypted data. The result of the operations is encrypted as well. A key field of application is the storage of sensitive (encrypted) data on a cloud server, where the result of a calculation is sent back to the owner of the data, also in encrypted form. The owner then has the private key to de-cypher the result and the cloud provider does neither know the data nor the result.[24] The crypto-systems are asymmetric, ie, public key cryptography.[25]

Let E() be the public ("external") part of an encryption function, D() the private or domestic part. Then, Figure 2 captures the concept of additive homomorphism. Homomorphically adding encrypted x and y (giving E(x) $\oplus$ E(y)) is identical to computing x+y and then encrypting the resulting sum. Operation $\oplus$ is the cryptographic equivalent of an addition.

Security, Scottsdale, Arizona, 3-7 November, USA: Association for Computing Machinery. Available from: http://dx.doi.org/10.1145/2660267.2660315 [Accessed 20 June 2025], pp. 703-715 and Bagnato, D. (2022). Recommendation CM/REC(2017)5 of the Council of Europe and an Analysis of eVoting Protocols. In: Kaiser, T. et al. (eds.) *CEEeGov 2022: Proceedings of the Central and Eastern European eDem and eGov Days*. Budapest, 22-23 September. USA: Association for Computing Machinery. Available from https://doi.org/10.1145/3551504.3551519 [Accessed 20 June 2025], pp. 169-178 and Karhumäki, J. and Meskanen, T. (2008). *Audit Report on Pilot Electronic Voting in Municipal Elections*, University of Turku, Turku

[23] State Electoral Office of Estonia (2016) *General Framework of Electronic Voting and Implementation thereof at National Elections in Estonia*, Tallinn. Available from: https://www.venice.coe.int/files/13EMB/13EMB_Priit_Vinkel.pdf [Accessed 20 June 2025]

[24] Gentry, C. (2010). *Computing Arbitrary Functions of Encrypted Data*. Communications of the ACM, Vol. 53(3). Available from: https://doi.org/10.1145/1666420.1666444 [Accessed 20 June 2025], pp. 97-105 and Gentry, C., Sahai, A. and Waters, B. (2013). Homomorphic Encryption from Learning with Errors: Conceptually-Simpler, Asymptotically-Faster, Attribute-Based. In: Canetti, R. and Garay, J.A. (eds.) CRYPTO 2013: Advances in Cryptology, *33rd Annual Cryptology Conference Proceedings*, Part I, Santa Barbara, 18-22 August. Germany: LNCS 8042. Available from: https://link.springer.com/chapter/10.1007/978-3-642-40041-4_5 [Accessed 20 June 2025], the authors also essentially contributed to the development of homomorphism in general.

[25] Salonaa A. (2013) *Public-Key Cryptography*. 2nd Ed., Berlin: Springer.

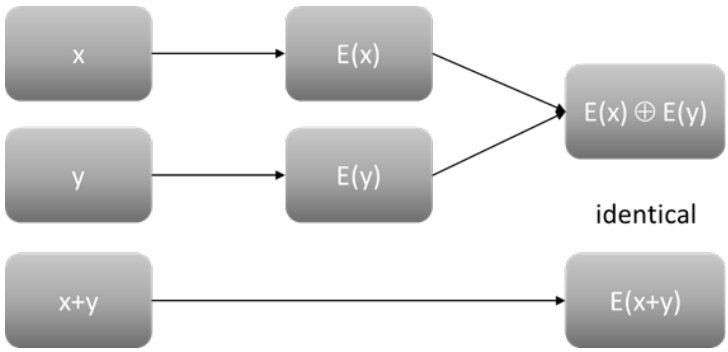

Figure 2: Additive homomorphism explained

Additive homomorphism readily lends itself to a homomorphic computation of an election result. Assume that the ballot consists of a single (yes/no or 1/0 question). Further assume three votes were cast and encrypted with E(), two of them "yes", one "no". Each vote is linked to the voter ID and the voter's digital signature ("outer envelope" in Figure 1). The homomorphic addition would then work as depicted in Figure 3.

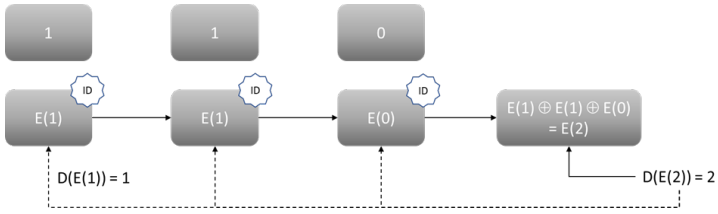

Figure 3: Casting and opening votes with homomorphic encryption

Homomorphic addition would yield E(2). Application of private key function D() yields the number of "yes" votes, i.e. the election result, by computing D(E(2)) = 2 without the necessity to decrypt ("open") the individual votes. But, and this is the main failure of this concept, you still need the private key to decipher the election results (here two "yes" votes). And once you have the domestic key D(), you may also decrypt each individual vote separately and thereby find out who voted for whom because the individual vote is linked to the voter ID. The unsolved problem here – and always when applying the envelope protocol - is that the individual votes which can be assigned to the voter still exist on the server of the election authority.

The addition of homomorphic encryption hence cannot solve the innate issues of envelope protocols. This result generally holds:

- Joint possession of the electronic ballot box and the private key of the election committee enables an attacker to break voting secrecy on a large scale;
- It also hinders to pass the ballot box on to a third party for an independent recount and keeping voter secrecy.

Hence, the violations of CM/Rec(2017)5 Standards 18, 19, 26 and, where applicable, Standard 25 mentioned in Section 2 a.-c. still apply. Therefore, by extension, also § 45 of the Social Code IV is not adhered to, as secrecy of the vote (Standards 19 and 26) and public reproducibility[26] (Standard 18) are not met.

4. EXTENSION 2: DIGITAL SIGNATURE KEY SURROGATE

Technical Guideline TR-03162, however, introduced another deviation from the Estonian system as it did not use digital signatures for the outer envelope. While digital signatures are extremely popular in Estonia, the digital signature is virtually non-existent in Germany and hence cannot be used for these purposes. TR-03162 therefore had to circumvent this issue. A recent press release of the Bundesdruckerei Group (100% state-owned former Federal Printing Office) stated that less than a fourth of the civil servants asked in a poll use digital signatures.[27] D-Trust, owned by Bundesdruckerei Group, recently published that only 16 % of the German companies use digital signatures,[28] hence the usage by private citizens cannot be significantly higher, rather the opposite. Unlike the Estonian ID[29], the German ID does not offer a digital signature, but it is only usable for identification purposes.[30]

[26] Cf. FN 21 concerning "Grundsatz der Öffentlichkeit der Wahl". If the election is not reproducible for an audit committee or court, it cannot possibly be reproducible for the general public.

[27] Cf. Bundesdruckerei GmbH (2023). *Volldigitale Prozesse in Behörden scheitern häufig an händischer Unterschrift*. [press release] 7 November. Available from: `https://www.presseportal.de/pm/14611/5643391` [Accessed 20 June 2025]

[28] Cf. Bundesdruckerei GmbH (2017). *Whitepaper: Durchgängig digital. mit Fernsignatur und elektronischem Siegel*. Available from: `https://www.d-trust.net/files/dokumente/pdf/whitepaper_fernsignatur_elektronisches_siegel.pdf` [Accessed 20 June 2025]

[29] e-Estonia. *E-Identity. ID-card* (n.d.). [online]. Available from: *https://e-estonia.com/solutions/e-identity/id-card/* [Accessed 20 June 2025]

[30] Bundesministerium des Inneren (2025) *Die elektronischen Funktionen des Personalausweises* [online] Available from: `https://www.personalausweisportal.de/Webs/PA/DE/`

It is the essence of the enveloping procedure to cast an authenticating digital signature on the encrypted ballot. In Sections 4.4f and particularly Figure 6, TR-03162 defines a surrogate for the usage of digital signatures.[31] Voters log into the election system using their Social Security Number, the last six digits of the backside of their eHealth Card[32] (both easily known to each medical service institution in Germany) plus the voter identification (Wahlkennzeichen, WKZ), which is an alphanumeric random character string issued for every voter in the roll and sent to voters by postal mail (2.2.1). Voters may also use their eID for login (4.4.2), but have to enter their WKZ anyway. Hence, the voter typically does not register by a strong means of identification (usage of the eID necessarily must be a minority programme), but by a character string sent by post. Hence, it is easy to intercept this letter and cast a vote on behalf of the voter if the above-mentioned six-digit social security number is known; it is also possible to collect WKZ. In our case, the demonstration and screenshots were produced using the data of the spouse of one of the authors – with her consent, but it would also have been technically possible to do that without her cooperation. According to Deutsches Ärzteblatt[33] the voter turnout at the elections was 11.5 million out of 55.3 million. This means that 43.8 million postal ballots were thrown into the wastebins and could have been used for electoral fraud.

A list of all generated WKZ is part of the election server system, however, has to be stored separately from the electronic ballot box (TR-03162, 2.2.2.4). After login, the usual voter checks are performed (eligible, has already cast a vote etc.). The following procedure to cast a vote is then performed (4.5.1 and 4.5.2 with Figures 6 and 7):

- The vote is encrypted with the public key of the election committee and sent to the election server without any authentication information (cf. Figure 4, Point 1).
- Upon receipt at the election server, the encrypted vote is signed by the election server and sent to the electronic ballot box. This is a

buergerinnen-und-buerger/der-personalausweis/funktionen/funktionen-node.html [Accessed 20 June 2025]

31 In the following, all section and figure references from TR-03162.

32 Note that the German Social Security Card is a chipcard, cf. Bundesministerium für Gesundheit (2024). *Elektronische Gesundheitskarte*. [press release] 5 December. Berlin. Available from: https://www.bundesgesundheitsministerium.de/themen/digitalisierung/elektronische-gesundheitskarte [Accessed 20 June 2025]. So a stronger identification could have been easily introduced.

33 Deutsches Ärzteblatt (2023). *Sozialwahl: Wahlbeteiligung trotz großer Kampagnen gesunken*. [online] Available from: https://www.aerzteblatt.de/news/sozialwahl-wahlbeteiligung-trotz-grosser-kampagnen-gesunken-07d62b7a-e6c0-401e-b4c8-107ed5835a90 [Accessed 20 June 2025]

clear surrogate to the vote-based signature in the "classical" Enveloping (Point 2). An advanced digital signature is permissible, a fully qualified digital signature is not required. An advanced signature does not require a qualified digital certificate nor a secure signature device.[34]

- This signed vote is then inserted in the electronic ballot box (Point 3).
- The WKZ is sent separately to another server to mark the WKZ as used; this entry must be stored without time stamp to avoid assignment to a vote according to the time the vote was signed and entered the ballot box. Interestingly, the voter login is not among the events to be protocolled either (2.4). Rather, TR-03162 explicitly rules out that insertion of a vote or insertion of a WKZ is logged (cf. Footnotes 9 and 10). It therefore must be noted that the election system cannot verify, when a voter (WKZ) voted.

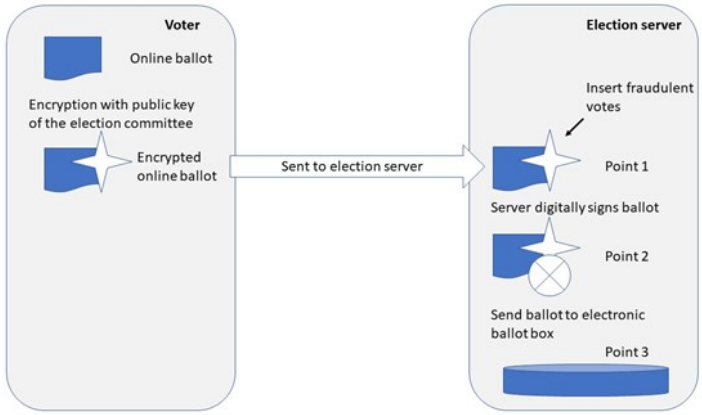

Figure 4: Voting procedure (derived from TR-03162, Figure 6, our translation and insertions)

Summarizing, the system design enables large-scale administrator fraud. The votes as received from the voters are encrypted with the public key of the election committee. The public key is, of course, known and a fraudulent election administration can insert votes and sign them.

[34] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. *Official Journal of the European Union* (L 257) 28 August. Available from: `https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014R0910` [Accessed 20 June 2025]

Submission of the WKZ and the vote are handled via two different "channels", ie, presumably two Web service addresses. There is no discernible mechanism to ensure that these two submissions are combined in a transaction (cf. ACID properties[35]). TR-03162 only states that if one fails, the event must be logged (4.5.2). What follows from that logging, is not specified.

In the counting stage, the signatures of the votes (by the election server) in the ballot box are verified and then either decrypted with the private key of the election committee or the result is homomorphically computed and the result is decrypted with that key. The ballots are then counted and the result established. In addition, the list of WKZ is checked and the sum of the WKZ and the sum of the votes are compared. TR-03162 also stipulates that the ballot box can be published. However, what would such a publication prove? It would merely show a list of ballots without any background information and the only validation would be the signature of the election server that could technically be faked by the server administration.

Let us now summarize the Sozialwahl eVoting in the light of Council of Europe Recommendation CM/Rec(2017)5 and mirror the technical properties of TR-03162 against selected standards in CM/Rec(2017)5. Standards quoted from the recommendation are depicted in italics.

5. SOZIALWAHL AND CM/REC(2017)5

The Social Election 2023 was in a Member State of the Council of Europe; hence the relevant recommendation of the Council of Ministers is fully applicable, despite its legally non-binding character, particularly in view of the stated "model character" of the eVoting.

The recommendation contains provisions for voting principles, any eVoting system used for political elections in a Member State must meet. The following chapter discusses, whether the system used in the German Social Election met these requirements, which were also required by the respective German law, § 45 (2) Social Code IV, or whether it violated them.

[35] As far as can be ascertained, the term goes back to: Haerder, T. and Reuter, A. (1983) Principles of transaction-oriented database recovery. *ACM Computing Surveys*, Vol. 15(4). Available from: `https://dl.acm.org/doi/10.1145/289.291` [Accessed 20 June 2025], pp. 287–317

5.1.SECRET SUFFRAGE

19. E-voting shall be organised in such a way as to ensure that the secrecy of the vote is respected at all stages of the voting procedure.

26. The e-voting process, in particular the counting stage, shall be organised in such a way that it is not possible to reconstruct a link between the unsealed vote and the voter. Votes are, and remain, anonymous.

As detailed in Section 2, the envelope procedure cannot fulfill these requirements[36].[37] Usage of a homomorphic encryption does not change this shortcoming as seen in Section 3. However, TR-03162 does not implement a classic envelope protocol. The vote is not signed by the voter, instead the WKZ is sent and stored separately from the vote (2.2.2.2); neither submission of the WKZ nor submission of the vote cast are logged. At first glance, voter secrecy appears to be ensured.

However, this is a web application, which must maintain its sessions, typically via cookies and the web application session referenced therein. Also, the vote must be included in a database representing the electronic ballot box. What does the ballot box table in that database look like? Does it have a primary key? If so, how is this key assigned? Typically, one would choose a random number or hexadecimal code and store the vote under that key. If that variant is chosen, there is a link Session – WKZ – ballot with assigned random key for database table TR-03162 appears to be aware of this issue, as it stipulates (our translation from the German original, Section 4.5.1):

"If the election platform maintains data during a processing, which enable a link between electronic vote, WKZ or identity of the voter, the election platform MUST

- Securely delete this data at the earliest possible stage, the latest however after conclusion of the transmission of the vote into the ballot box and
- Secure via technical/organisational measures that access to this data is only available via the election platform."

Therefore, the fundamental issues with envelope procedures may appear again in this scaled-down version of the protocol. Again, homomorphic encryption does not solve the issue. Note that the deletion of the data may fulfil the requirement for secret suffrage, but violates the auditability, both listed in § 45 (2) Social Code IV. Such a violation cannot be accepted "with a view to the technical features also at the online elections", as § 194a (4)

[36] Bagnato, D. (2022) Recommendation CM/REC(2017)5 of the Council of Europe and an Analysis of eVoting Protocols. *op. cit.*

[37] Prosser, A. (2014) Transparency in eVoting - Lessons learnt. *Transforming Government: People, Process and Policy*, 8(2), pp. 171-184

would suggest, at least not within the standards established by the Council of Europe[38].

5.2.FREE SUFFRAGE

15. The voter shall be able to verify that his or her intention is accurately represented in the vote and that the sealed vote has entered the electronic ballot box without being altered. Any undue influence that has modified the vote shall be detectable.

16. The voter shall receive confirmation by the system that the vote has been cast successfully and that the whole voting procedure has been completed.

17. The e-voting system shall provide sound evidence that each authentic vote is accurately included in the respective election results. The evidence should be verifiable by means that are independent from the e-voting system.

18. The system shall provide sound evidence that only eligible voters' votes have been included in the respective final result. The evidence should be verifiable by means that are independent from the e-voting system.

Apart from Standard 16, the system specified in TR-03162 does not fulfill any of these properties. The vote bears no authentication beyond the digital signature of the election server. Unlike in the Estonian system one cannot establish that the vote was cast by an eligible voter (the digital signature of the voter in the outer envelope). All this system can establish is the evidence that the vote was signed by the election system itself. There is no link to a WKZ or any other authentication information beyond that. Hence, the voter cannot verify that her vote was stored and counted as cast. Ex post publication of the ballots does not change this. All the system described in TR-03162 can verify is:

- There are as many WKZ as there are votes;
- All votes in the ballot box have been correctly signed by the election server;
- All votes have been cast in the election period.

[38] see Standard 39 below

5.3.ACCOUNTABILITY

39. The e-voting system shall be auditable. The audit system shall be open and comprehensive, and actively report on potential issues and threats.

The system described in TR-03162 can detect illicit access to election master data, such as the voter roll or the WKZ. However, there is no audit chain possible that establishes that:

- The vote was cast by an eligible voter;[39]
- The vote was inserted in the ballot box as cast by the eligible voter.[40]

The system described in TR-03162 is therefore not auditable. This view is also shared by the official audit report[41], which was published in late 2024, after the submission of this paper to MUJLT (p.42, our translation from German):

[The independent expert verifying the result] arrived at the conclusion that the auditability of the election technology employed for the Sozialwahl could not be ascertained, as the definition of the cryptographic protocol and the source code showed issues that prevented the auditability of the election result.

The "issues" leading to this assessment are not technically detailed in the audit report but will most likely be the ones listed above.

6. CONCLUSION

This paper analysed an eVoting system used for the German Social Elections in 2023, particularly the underlying Technical Guideline TR-03162. The system implements a classical envelope procedure with two major deviations: usage of homomorphic encryption and non-usage of digital signatures by the voter on the outer envelope of the vote with the WKZ mechanism as a substitute.

The paper established the following results in view of CM/REC(2017)5:

1. Use of homomorphic encryption does not solve the fundamental issues of Enveloping as the fact remains that voter identification data and (encrypted) vote are stored in the ballot box. Once the private key of the election committee has been provided, it can be used to decipher the connection voter – vote. This violated Standards 19 and 26.

[39] See argument in 5.2

[40] See argument in 5.2

[41] KPMG (2024) *Evaluierung des Modellprojekts zur Durchführung von Online-Wahlen bei den Krankenkassen nach § 194d SGB V*. Report from 30 October. Available from: `https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/5_Publikationen/Ministerium/Berichte/Abschlussbericht_Evaluation_Modellprojekt_Online-Wahlen.pdf` [Accessed 20 June 2025]

2. Addition of an artificial voter identifier (WKZ) instead of a digital signature of the voter (as in the Estonian "original" of the protocol) creates a whole host of auditability and verification issues. It enables large-scale administrator fraud. The protocol variant chosen for the Sozialwahl hence neither enables individual auditability by the voter nor general auditability in an independent recount. Also in this regard, the protocol addition does not solve the inherent auditability issue of the Envelope protocol violating Standards 15, 17, 18 and 39.
3. An artificial identifier like WKZ does not guarantee voter secrecy either, as the link voter – vote may be reconstructed by session data maintained by the servers involved violating Standards 19 and 26.
4. It was shown that the protocol chosen violated a number of major standards of Recommendation CM/REC(2017)5. Given that this eVoting was described as a "model project" in the relevant Decree, one can only strongly recommend that this system is never rolled out for real political elections.

The voter turnout showed that the eVoting pilot was no game changer: According to the Federal Election Commissioner for the Social Election 334,166 voters choose online voting, the portion of the total votes cast being between 2.42 % (DAK-Gesundheit) and 9.96 % (Techniker Krankenkasse). Techniker Krankenkasse, the one with the highest eVoting turnout, lost 380,590 voters in total despite 200,080 eVoters. eVoters totalled for 334,166 votes while the loss in total votes cast was 3,836,580.[42]

LIST OF REFERENCES

[1] Bagnato, D. (2022). Recommendation CM/REC(2017)5 of the Council of Europe and an Analysis of eVoting Protocols. In: Kaiser, T. et al. (eds.) *CEEeGov 2022: Proceedings of the Central and Eastern European eDem and eGov Days*. Budapest, 22-23 September. USA: Association for Computing Machinery. Available from `https://doi.org/10.1145/3551504.3551519` [Accessed 20 June 2025], pp. 169-178.

[2] Balthasar, A. and Prosser, A. (2012). E-Voting in der Sonstigen Selbstverwaltung - Anmerkungen zu VfGH vom 30. Juni 2011, B 1149, und vom 13. Dezember 2011, V 85-96. *Journal für Rechtspolitik (JRP)*, 2012(1), pp. 47-86.

[42] KPMG (2024) Evaluierung des Modellprojekts zur Durchführung von Online-Wahlen bei den Krankenkassen nach § 194d SGB V. *Op. cit.*

[3] Bundesamt für Sicherheit in der Informationstechnik (2023). *Technische Richtlinie TR-03162, Version 1.3, 3.2.2023.* Bonn. In German. Available from: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03162/TR-03162_node.html#:~:text=Die\%20Technische\%20Richtlinie\%20TR\%20\%2D03162,Briefwahl\%20auch\%20Online\%2DWahlen\%20anzubieten [Accessed 20 June 2025].

[4] Bundesdruckerei GmbH (2017). *Whitepaper: Durchgängig digital. mit Fernsignatur und elektronischem Siegel*. Available from: https://www.d-trust.net/files/dokumente/pdf/whitepaper_fernsignatur_elektronisches_siegel.pdf [Accessed 20 June 2025].

[5] Bundesdruckerei GmbH (2023). *Volldigitale Prozesse in Behörden scheitern häufig an händischer Unterschrift*. [press release] 7 November. Available from: https://www.presseportal.de/pm/14611/5643391 [Accessed 20 June 2025].

[6] Bundesministerium des Inneren (2025) *Die elektronischen Funktionen des Personalausweises* [online] Available from: https://www.personalausweisportal.de/Webs/PA/DE/buergerinnen-und-buerger/der-personalausweis/funktionen/funktionen-node.html [Accessed 20 June 2025].

[7] Bundesministerium für Arbeit und Sozialordnung (1997). *Wahlordnung für die Sozialversicherung* (Election Decree for the Social Elections). In German. Available from: https://www.gesetze-im-internet.de/svwo_1997/ [Accessed 20 June 2025].

[8] Bundesregierung (2023) *Wissenswertes zur Sozialwahl 2023*. [online] Berlin. Available: https://www.bundesregierung.de/breg-de/aktuelles/sozialwahl-2023-2188062 [Accessed 20 July 2025].

[9] Council of Europe (2017). *Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting*, Strasbourg. Available from: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=0900001680726f6f [Accessed 28 March 2025].

[10] Der Bundeswahlbeauftragte für die Sozialversicherungswahlen (2024). *Schlussbericht des Bundeswahlbeauftragten für die Sozialversicherungswahlen zu den Sozialwahlen 2023*. Final Report of the Federal Election Commissioner for the Social Election. Berlin: Bundesministerium für Arbeit und Soziales. Available from: https://www.bmas.de/SharedDocs/Downloads/DE/Meldungen/2024/bundessozialwahl-2023-schlussbericht.pdf?__blob=publicationFile&v=1 [Accessed 20 June 2025].

[11] Deutsches Ärzteblatt (2023). *Sozialwahl: Wahlbeteiligung trotz großer Kampagnen gesunken*. [online] Available from: https://www.aerzteblatt.de/news/sozialwahl-wahlbeteiligung-trotz-grosser-kampagnen-gesunken-07d62b7a-e6c0-401e-b4c8-107ed5835a90 [Accessed 20 June 2025].

[12] e-Estonia. *E-Identity. ID-card* (n.d.). [online]. Available from: *https://e-estonia.com/solutions/e-identity/id-card/* [Accessed 20 June 2025].

[13] Estonian National Electoral Committee (2010). *E-Voting System, General Overview*, Tallinn. Available from: https://www.valimised.ee/sites/default/files/uploads/eng/General_Description_E-Voting_2010.pdf [Accessed 20 June 2025].

[14] Federal Ministry of Health (2020). *Verordnung über die technischen und organisatorischen Vorgaben für die Durchführung einer Online-Wahl im Rahmen des Modellprojekts nach § 194a des Fünften Buches Sozialgesetzbuch*. Berlin. In German. Available from: https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/3_Downloads/Gesetze_und_Verordnungen/GuV/O/Online-Wahl-VO_Bgbl.pdf [Accessed 20 June 2025].

[15] Federal Office for Information Security (2018). *Guide to Basic Protection based on IT-Grundschutz*. Bonn. In German. Available from: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/Basic_Security.html?nn=908032 [Accessed 20 June 2025].

[16] Gentry, C. (2010). *Computing Arbitrary Functions of Encrypted Data*. Communications of the ACM, Vol. 53(3). Available from: https://doi.org/10.1145/1666420.1666444 [Accessed 20 June 2025], pp. 97-105.

[17] Gentry, C., Sahai, A. and Waters, B. (2013). Homomorphic Encryption from Learning with Errors: Conceptually-Simpler, Asymptotically-Faster, Attribute-Based. In: Canetti, R. and Garay, J.A. (eds.) CRYPTO 2013: Advances in Cryptology, *33rd Annual Cryptology Conference Proceedings*, Part I, Santa Barbara, 18-22 August. Germany: LNCS 8042. Available from: https://link.springer.com/chapter/10.1007/978-3-642-40041-4_5 [Accessed 20 June 2025].

[18] GKV Spitzenverband. *Die gesetzlichen Krankenkassen*. [online] Bonn. Available from: https://www.gkv-spitzenverband.de/krankenversicherung/kv_grundprinzipien/alle_gesetzlichen_krankenkassen/alle_gesetzlichen_krankenkassen.jsp [Accessed 19 June 2025].

[19] Haerder, T. and Reuter, A. (1983) Principles of transaction-oriented database recovery. *ACM Computing Surveys*, Vol. 15(4). Available from: https://dl.acm.org/doi/10.1145/289.291 [Accessed 20 June 2025], pp. 287–317.

[20] Huber, N. et al. (2022). Kryvos: Publicly Tally-Hiding Verifiable E-Voting. In: Yin, H. and Stavrou, A. (eds.) *CCS 2022: Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, Los Angeles, 7 Nov. USA: Association for Computing Machinery. Available from: https://doi.org/10.1145/3548606.3560701 [Accessed 20 June 2025], pp. 1443–1457.

[21] Karhumäki, J. and Meskanen, T. (2008). *Audit Report on Pilot Electronic Voting in Municipal Elections*, University of Turku, Turku.

[22] KPMG (2024) *Evaluierung des Modellprojekts zur Durchführung von Online-Wahlen bei den Krankenkassen nach § 194d SGB V*. Report from 30 October. Available from: https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/5_Publikationen/Ministerium/Berichte/Abschlussbericht_Evaluation_Modellprojekt_Online-Wahlen.pdf [Accessed 20 June 2025].

[23] Nakielski, H. (2022). *Gerichte und Richter:innen der Sozialgerichtsbarkeit*. [online]. Available from: https://netzwerk-sozialrecht.net/gerichte-und-richterinnen-der-sozialgerichtsbarkeit/ [Accessed 20 June 2025].

[24] Bundesministerium für Gesundheit (2024). *Elektronische Gesundheitskarte*. [press release] 5 December. Berlin. Available from: https://www.bundesgesundheitsministerium.de/themen/digitalisierung/elektronische-gesundheitskarte [Accessed 20 June 2025].

[25] Peng, K. and Bao, F. (2009). A Design of Secure Preferential E-Voting. In: Ryan, P.Y.A. and Schoenmakers, B. (eds.) *Vote-ID 2009: International Conference on E-Voting and Identity*, Luxembourg, 7-8 September. Germany: LNCS 5767. Available from: https://link.springer.com/chapter/10.1007/978-3-642-04135-8_9 [Accessed 20 June 2025], pp. 141-156.

[26] Prosser, A. (2004) Implementation of Quorum-Based Decisions in an Election Committee. In: Traunmüller, R. (ed.) *DEXA/EGOV 2004: 15th International Workshop on Database and Expert Systems Applications*, Zaragossa, 30 August – 3 September. Germany: LNCS 3183, pp. 122-127.

[27] Prosser, A. (2014) Transparency in eVoting - Lessons learnt. *Transforming Government: People, Process and Policy*, 8(2), pp. 171-184.

[28] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. *Official Journal of the European Union* (L 257) 28 August. Available from: https://eur-

lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014R0910 [Accessed 20 June 2025].

[29] Rivest, R. L., Shamir, A., and Adleman, L. (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM, 21(2)*, Available from: https://dl.acm.org/doi/pdf/10.1145/359340.359342 [Accessed 20 June 2025], pp. 120-126.

[30] Salonaa A. (2013) *Public-Key Cryptography*. 2nd Ed., Berlin: Springer.

[31] *Sozialgesetzbuch (SGB) Fünftes Buch (V) - Gesetzliche Krankenversicherung* - (Artikel 1 des Gesetzes v. 20. Dezember 1988, BGBl. I S. 2477) (Social Code V). In German. Available from: https://www.gesetze-im-internet.de/sgb_5/ [Accessed 20 June 2025].

[32] *Sozialgesetzbuch (SGB) Viertes Buch (IV) - Gemeinsame Vorschriften für die Sozialversicherung* - (Artikel I des Gesetzes vom 23. Dezember 1976, BGBl. I S. 3845) (Social Code IV). In German. Available from: https://www.gesetze-im-internet.de/sgb_4/ [Accessed 20 June 2025].

[33] Springall, D. et al. (2014). Security Analysis of the Estonian Internet Voting System. In: *CCS'14: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communication Security*, Scottsdale, Arizona, 3-7 November, USA: Association for Computing Machinery. Available from: http://dx.doi.org/10.1145/2660267.2660315 [Accessed 20 June 2025], pp. 703-715.

[34] State Electoral Office of Estonia (2016) *General Framework of Electronic Voting and Implementation thereof at National Elections in Estonia*, Tallinn. Available from: https://www.venice.coe.int/files/13EMB/13EMB_Priit_Vinkel.pdf [Accessed 20 June 2025].