The Council of Europe's CM/Rec(2017)5 on e-voting and Secret Suffrage: Time for yet Another Update?

Adrià Rodríguez-Pérez[1,2](✉)

[1] Scytl Election Technologies, S.L.U, 08021 Barcelona, Spain
adria.rodriguez@scytl.com
[2] Universitat Rovira i Virgili, 43002 Tarragona, Spain

Abstract. The Council of Europe's Recommendation CM/Rec(2017)5 on e-voting remains the main international legal standard in the field. According to the updated Recommendation, e-voting should respect all the principles for democratic elections. This includes, of course, the principle of secret suffrage. Provisions on secret suffrage are dispersed throughout Rec(2017)5 and its related documents. The main provisions can be found in Section IV of Appendix I, but the principle is also mentioned in several other sections, in the Explanatory Memorandum, and in the Guidelines. A detailed analysis of all these provisions reveals important flaws in the understanding of secret suffrage in (remote) e-voting. Some of the flaws are the result of an inaccurate understanding of secret suffrage, in which this principle is mixed with provisions on personal data protection. In other cases, the flaws are due to analogies being drawn with paper-based voting channels, which prevent the standards from taking stock of the specificities of (remote) e-voting. In this paper I provide a detailed account of these flaws. I also suggest some alternative approaches and wording for the provisions on secret suffrage. Lastly, I discuss the desirability and feasibility of different alternatives regarding the review of Rec(2017)5.

Keywords: Remote electronic voting · International standards · Secret suffrage

1 Introduction

The Council of Europe's Recommendation CM/Rec(2017)5 on e-voting remains the main international legal standard in the field. According to the updated Recommendation, e-voting should respect all the principles for democratic elections (Council of Europe 2017a: para. i). This includes, of course, the principle of secret suffrage: one of the five principles of the European Electoral Heritage, according to the Venice Commission's Code of Good Practice in Electoral Matters (2002). Provisions on secret suffrage are dispersed throughout Re(2017)5 and its related documents: the Explanatory Memorandum and the Guidelines. The main provisions can be found in Section IV of Appendix I, but the principle is also mentioned in several other sections, either directly or indirectly.

R. Krimmer et al. (Eds.): E-Vote-ID 2022, LNCS 13553, pp. 90–105, 2022.
https://doi.org/10.1007/978-3-031-15911-4_6

A detailed analysis of all these provisions reveals important flaws in the understanding of secret suffrage in (remote) electronic voting.

In this paper, I provide a detailed account of these flaws. I also suggest some alternative approaches and wording for the provisions on secret suffrage in the Recommendation. Lastly, I discuss the desirability and feasibility of different alternatives regarding the review of Rec(2017)5. The focus of the paper is on remote e-voting[1] technologies. These can take many forms and shapes, but they share one characteristic: the devices used to vote (be it a computer or a laptop, a smartphone or even a smart TV) are located remotely from the voting or counting servers, and the connection between the two depends upon the Internet as the voting channel. Because it is remote, internet voting opens the door to voting from uncontrolled environment, raising concerns about the secrecy of the vote.

The next section provides a brief introduction to the Council of Europe's recommendations on e-voting. The goal is to understand the drivers behind the adoption of these standards and their recent update. In Sect. 3, I look more specifically into the provisions on secret suffrage in the updated Recommendation. I look directly at the standards on secret suffrage, but at the same time I also describe direct and indirect references to this principle throughout the Recommendation. Lastly, Sect. 4 addresses the issue at stake: is it necessary to update Rec(2017)5? I suggest two different issues that should be taken into account regarding the current standards. On the one hand, the scope of the provisions on secret suffrage needs to be revisited. The current provisions mix secret suffrage with personal data protection, which is inaccurate. On the other hand, many of the provisions in the Recommendation are still largely based on how secret suffrage is understood in paper-based elections. I argue that in contrast to the aims behind the update, several provisions still fail at specifying how secret suffrage must be protected in (remote) e-voting. Following, the conclusions provide a summary of the main findings and recommendations in the paper.

2 The Council of Europe's Rec(2017)5

To date, the Council of Europe's standards on e-voting remain the main intergovernmental source in the field. While not binding, the Council of Europe's Recommendations have been voluntarily adopted by several member States of the Council of Europe, including Norway (Barrat et al. 2012; Driza Maurer 2014: 112; Stein and Wenda 2014: 106) and Switzerland (Swiss Federal Council 2013: 46). In Estonia, the Supreme Court has also referred to it and in Belgium the Recommendations have been used as a benchmark when evaluating e-voting (Stein and Wenda 2014: 106). For this reason, Robert Stain and Gregor Wenda have argued that the Recommendation "has been the most relevant international document and reference regarding e-voting" (2014: 105). More recently, Ardita Driza Maurer has also acknowledged that "[t]he Council of Europe is the only international organization to have issued recommendations on the regulation of the use of e-voting" (2017: 146). In this section, I look at the origins of the Recommendation, its update, and the main drivers behind this effort. The goal is to understand why and

[1] I use indistinguishably the terms "remote electronic voting", "internet voting", and "online voting" (also in their shorter versions as "remote e-voting" or "i-voting") to refer to e-casting technologies used from remote environments, both controlled and uncontrolled.

how the Recommendation has been updated before looking into its provisions on secret suffrage with more detail.

2.1 The First Council of Europe's Standards on e-voting

The origins of the Recommendation date back to the early 2000. At the initiative of some member states, the Committee of Ministers of the Council of Europe set up a group of experts and adopted, on 30 September 2004, a recommendation on legal, operational and technical requirements for e-voting: Rec(2004)11 (Council of Europe 2004a, b).

Drawing from various regulations governing elections and voting in the Council of Europe's member States, the recommendation only set minimum standards. The 2004 recommendation stressed that "e-voting shall respect all the principles for democratic elections and referendums" (Council of Europe 2004a: i) and "shall be as reliable and secure as democratic elections and referendums which do not involve the use of electronic means" (Council of Europe 2004a: i). Additional guidelines were adopted regarding the certification of remote electronic voting systems (Council of Europe 2010a) and the transparency of e-enabled elections (Council of Europe 2010b), as well as an E-voting handbook on the "key steps in the implementation of e-enabled elections" (Stein and Wenda 2014: 105).

Ten years after its adoption, however, "voices in favour of a formal update […] gained strength" (Stein and Wenda 2014: 105). For instance, in their evaluation of the Norwegian experience against the 2004 Recommendation, Jordi Barrat i Esteve and Ben Goldsmith concluded that "[t]he recommendations [sic] do not build on existing public international law […] say little on the legal basis, trying, on the contrary, to cover every possible situation in a technically neutral way. The consequence is sometime vague wording that makes the enforcement of the recommendation more difficult than it should be" (2012: 8). Additionally, Ardita Driza Maurer (2014: 113) also takes note of criticism coming from Douglas Jones (2004), from Margaret McGaley and J. Paul Gibson (2006), and from Andreas Ehringfeld et al. (2010).

2.2 The Road Towards Updated Rec(2017)5

Therefore, "[f]ollowing an informal experts' meeting in Vienna on 19 December 2013, the Committee of Ministers was confronted with the suggestion to formally update the Recommendation in order to keep up with the latest technical, legal and political developments" (Stein and Wenda 2014: 105). It was argued that "[n]ew technological developments and concepts such as in the context of the verifiability of votes, and conclusions from studies and reports, for instance regarding certification, called for addenda or adaptations" (Stein and Wenda 2014: 107).

A study commissioned to Ardita Driza Maurer (2015), and based on a survey among election administrations in the member states of the Council of Europe, identified the following items within the scope of the update: (1) the definition of e-voting, (2) the responsibilities of Electoral Management Bodies, (3) the notion of risk, (4) the structure of the Recommendation, and (5) the categories of requirements. New standards were drafted and approved by an Ad hoc Committee of Experts on Legal, Operational and Technical Standards for e-voting (CAHVE) in November 2016 (Driza Maurer 2017: 147). The

Committee of Ministers of the Council of Europe finally adopted the updated standards as Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting on 14 June 2017.

The current definition has been broadened to include e-voting as well as counting machines. Regarding its structure, the current Recommendation consists of three documents: "the Recommendation, which outlines central aspects of e-voting; an Explanatory Memorandum; and guidelines to inform the implementation of provisions in the Recommendation" (Essex and Goodman 2020: 169). Another important innovation is that the Recommendation also introduces the notion of risk. In this sense, "Recommendation ii. Stresses the need to assess risks, namely those specific to e-voting and to adopt appropriate measure to counter them" (Driza Maurer 2017: 154).

Notwithstanding, possibly the most important change in Rec(2017)5 refers to its approach towards e-voting. While the 2004 Recommendation stated that "[e]-voting shall be as reliable and secure as democratic elections and referendums which do not involve the use of electronic means" (Council of Europe 2004a: i), the updated recommendation has dropped this previous comparison (Driza Maurer 2017: 154). The benchmark in Rec(2017)5 "is [the] respect for all principles of democratic elections and referendums" (Driza Maurer 2017: 154). In practice, it means that "standards should be derived directly from the applicable principles" (Driza Maurer 2017: 154).

Since their adoption, the new standards have been welcomed both by members and non-Members states of the Council of Europe. For example, in the explanatory report to the draft law amending the Federal Act on Political Rights, the Swiss Federal Chancellery referenced the updated Recommendation (2018: 22). They argued that the draft legislation was in line with the provisions of the updated Recommendation on verifiability, certification, and risk management. Elsewhere, Aleksander Essex and Nicole Goodman (2020) have been quick to assess to what extent the Council of Europe's approach to regulating e-voting could work in Canada.

3 Secret Suffrage in Rec(2017)5

Therefore, the Council of Europe's Recommendation Rec(2017)5 on e-voting remains the main international legal standard in the field. Having set the stage with the description of its background and update effort, this section will focus more specifically on its provisions on secret suffrage.

The Recommendation offers a definition of secret suffrage in its Explanatory Memorandum. Based on the Venice Commission's Code of Good Practice in Electoral Matters (2002), secret suffrage is summarised as "the voter has the right to vote secretly as an individual, and the state has the duty to protect that right" (Council of Europe 2017b: para. 14). The Recommendation then identifies a set of standards to fulfil this principle. In what follows, I analyse these standards separately. First, I address those standards that are directly related to secret suffrage, which in the Recommendation are included in Section IV of Appendix I. Second, I identify some additional references to secret suffrage throughout the Recommendation and its additional documents.

3.1 Secret Suffrage: Section IV

Section IV in the first Appendix to the Recommendation is entitled secret suffrage and identifies eight standards related to this principle (standards 19 to 26).

The first of these standards provides a general overview about how (remote) e-voting systems must comply with secret suffrage. In this sense, standard No. 19 reads that "[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" (Council of Europe 2017a). This is an umbrella provision on secret suffrage that "sets the general requirement for secrecy of the vote which applies throughout the entire procedure" (Council of Europe 2017b: para. 63). On the one hand, it references "encryption" (Council of Europe 2017b: para. 64), which is a mean to ensure the confidentiality of the vote. On the other, it also notes "that the votes cast are mixed in the electronic ballot box so the order in which they appear at the counting phase does not allow reconstruction of the order in which they arrived" (Council of Europe 2017b: para. 64) as a mechanism to ensure anonymity.

Following, standard No. 20 provides that "[t]he e-voting system shall process and store, as long as necessary, only the personal data needed for the conduct of the e-election" (Council of Europe 2017a). Standards No. 21 and 22 deal with authentication data and voter's registers, respectively, and not with the right to vote secretly. As I will argue below (Sect. 4.1), secret suffrage is different from personal data protection, and therefore these standards should have not been included under Section IV.

Section IV further details four additional standards, on: receipt-freeness (standard No. 23), election fairness (standard No. 24), a provision about the secrecy of previous choices (standard No. 25), and anonymity (standard No. 26). These standards are indeed all related to secret suffrage and touch upon some of the key concerns about secret suffrage in (remote) e-voting.

Standard No. 23 reads that "[a]n e-voting system shall not provide the voter with proof of the content of the vote cast for use by third parties" (Council of Europe 2017a). According to the Explanatory Memorandum, "[t]he aim of this standard is to prevent the breach of vote secrecy as well as vote selling" (Council of Europe 2017b: 70). This standard has been reviewed, corrected, and clarified from the previous Recommendation (Driza Maurer 2017: 155).

According to standard No. 24, "[t]he e-voting system shall not allow the disclosure to anyone of the number of votes cast for any option until after the closure of the electronic ballot box. This information shall not be disclosed to the public after the end of the voting period" (Council of Europe 2017a).

Standard No. 25 reads that "[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" (Council of Europe 2017a: 6). Therefore, standard No. 25 extends the reach of confidentiality to the "previous choices recorded and erased by the voter before issuing his or her final vote" (Council of Europe 2017a) and granting them "the same protection as the secrecy of the final vote" (Council of Europe 2017b: para. 76). This is important because it highlights certain requirements that may have to be put in place specifically for (remote) e-voting.

Lastly, standard No. 26 reads that "[t]he 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" (Council of Europe 2017a: 6).

3.2 Beyond Section IV

Direct References. In addition to the standards which fall all directly under section IV on secret suffrage, the Recommendation also touches upon this principle in regard to standards No. 44, No. 45, and No. 46.

First, standard No. 44 reads that "[i]f stored or communicated outside controlled environments, the votes shall be encrypted" (Council of Europe 2017a). Since this analysis focuses on i-voting (from uncontrolled environments), this standard fully applies. Second, standard No. 45 can be linked to confidentiality and anonymity. This standard sets that "[v]otes and voter information shall be kept sealed until the counting process commences" (Council of Europe 2017a). Therefore, this standard "clarifies the moment where [sic] sealing ends" (Council of Europe 2017b: para. 45).

Lastly, standard No. 46 provides that "[t]he electoral management body shall handle all cryptographic material securely" (Council of Europe 2017a: 8). This provision is key, not only because it is necessary to efficiently guarantee most of the provisions related to secret suffrage, but also because it draws attention to the relevance of operational measures. In this sense, the key-distribution mechanisms described in the Guidelines for the implementation of this standard (Council of Europe 2017c) are of paramount importance to ensure that the confidentiality and anonymity of the votes are preserved. On top of that, this Guideline acknowledges as well that "[t]he private cryptographic keys be [sic] should be generated at a public meeting" (Council of Europe 2017c), bridging the principle of secret suffrage with the requirements for transparency and observation.

Indirect References. Indirect references to secret suffrage can be found in standards No. 6 (related to equal suffrage), in standards No. 16 to No. 18 (in relation to free suffrage), and in standard No. 40 (related to the reliability of the system). While none of those standards deals in principle with secret suffrage, neither directly or indirectly, they reference this principle either in the provisions of the Explanatory Memorandum or in the Guidelines.

Secret and Free Suffrage. Overall, the Explanatory Memorandum and the Guidelines for the standards on free suffrage detail that their provisions should be balanced against the requirements for secret suffrage. More specifically, these standards highlight the need to balance the transparency and auditability of the election with the protection of secret suffrage. First, standard No. 16 reads that "[t]he voter shall receive confirmation by the system that the vote has been cast successfully and that the whole voting procedure has been completed" (Council of Europe 2017a). This provision is completed in the Explanatory Memorandum to the Recommendation, which reads that "[i]t is good practice to accompany these messages with a reminder and instructions to the voter on how to delete traces of the vote if voting was done from an uncontrolled device" (Council of Europe 2017b: para. 58).

Second, standard No. 17 provides that “[t]he 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” (Council of Europe 2017a). For this standard, the Explanatory Memorandum to the Recommendation reads that “it should be possible to audit the evidence to verify its correctness with tools which are external and independent from the e-voting system. To do so, the e-voting system should provide interfaces with comprehensive observation and auditing possibilities, subject to the needs of secrecy and anonymity of the vote” (Council of Europe 2017b: para. 60).

Third, standard No. 18 notes that “[t]he 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” (Council of Europe 2017a). For this standard, the Explanatory Memorandum to the Recommendation adds that “[v]oters and third parties should be able to check that only eligible voters’ votes are included in the election result. At the same time counted votes should be anonymous. In the case of internet voting, there exist encryption methods that do not require decoding before votes are counted (homomorphic encryption). Counting can be performed without disclosing the content of encrypted votes” (Council of Europe 2017b: para. 62).

Secret and Equal Suffrage. Provisions on standard No. 6 also call for taking into account the principle of secret suffrage. More specifically, the standard states that “[w]here electronic and non-electronic voting channels are used in the same election or referendum, there shall be a secure and reliable method to aggregate all votes and to calculate the results” (Council of Europe 2017a: 5). In turn, the Explanatory Memorandum to the Recommendation sets that “[w]hen the number of e-votes or of paper votes is particularly small there is the risk that vote secrecy may be violated if the results of those few votes are disclosed. The aggregation method should contain the necessary technical and procedural safeguards to ensure the consolidation of results of the different voting channels before results are disclosed, thus ensuring secrecy. In addition, procedural rules, related namely to personnel intervening in the counting process, should take into account such cases” (Council of Europe 2017b: para. 7).

Secret Suffrage and the Reliability of the System. Lastly, standard No. 40 prescribes that “[t]he electoral management body shall be responsible for the respect for and compliance with all requirements even in the case of failures and attacks. The electoral management body shall be responsible for the availability, reliability, usability and security of the e-voting system” (Council of Europe 2017a). This is an umbrella provision regarding the obligations of election administrations when they introduce (remote) e-voting, which obviously also includes compliance with secret suffrage. The provisions about this standard in the Guidelines will be discussed further in Sect. 4.2. Below.

4 Time for yet Another Update?

Based on the analysis conducted in the previous section, I am of the opinion that not sufficient effort has been put into directly deriving the standards in Appendix I.IV of the Recommendation from the principle of secret suffrage. More specifically, I have identified two fundamental flaws. The first one is linked to the scope of secret suffrage in the Recommendation. In this regard, including data protection provisions under the scope of this principle is totally inadequate because not all personal data processed in an election is related to the secrecy of the vote. Second, and more importantly, the provisions on secret suffrage are still largely based on how this principle is understood in paper-based elections. For this reason, in this section I suggest a new scope and approach to regulate secret suffrage in the Council of Europe's Rec(2017)5.

4.1 The Need for a Clearer Scope

The need for a clearer scope becomes obvious if one takes into account that the provisions in the Recommendation mix the standards of secret suffrage with those of personal data protection. Secondly, some of the Guidelines also seem to point towards an understanding of secret suffrage as being a means to achieve other principles. However, provisions under Appendix I.IV of the Recommendation should all have secret suffrage as an end in itself.

Secret Suffrage and Personal Data Protection. First and foremost, and as I have previously argued (Rodríguez-Pérez 2020: 175), including data protection provisions under the umbrella of secret suffrage is totally inadequate. Votes may be considered personal data in certain circumstances, but personal data is much broader than the legal assets protected by secret suffrage. Therefore, standards No. 20, No. 21, and No. 22 should be moved to another section in the Appendix.

The flawed understanding of the links between secret suffrage and personal data protection can be found in the Explanatory Memorandum. In standard No. 20, the Explanatory Memorandum to the Recommendation specifies that "[d]ata minimisation aims at ensuring data protection and is part of vote secrecy" (Council of Europe 2017b: para. 65). However, secret suffrage and personal data protection are complementary regulations, sometimes overlapping, but under no circumstances one is "part of" the other.

Personal data is much broader than any data that may fall under the scope of secret suffrage. For example, art. 4(1) of the European Union's General Data Protection Regulation (GDPR) defines personal data as "any information relating to an identified or identifiable natural person ('data subject')". Similarly, the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data also defines it as "any information relating to an identified or identifiable individual" (art. 2.a).

As a result, personal data protection regulations apply as well to personal data processed about voters, candidates, and even members of the election administration or election observers (Rodríguez-Pérez 2020: 173–175): their names, addresses and contact details, the fact that they belong to a political party or a civil society organisation, etc. are all personal data. In contrast, secret suffrage would deal only with the contents of the vote cast and the conditions in which voters cast them. Thus, data protection is in fact broader than vote secrecy (some aspects of data protection do not deal with the vote at all) and cannot be "part of" it. There is no room for standards No. 20, No. 21 and No. 22 under the provisions on secret suffrage in Appendix I.IV.

On the Publication of Preliminary Results and Secret Suffrage. Standard No. 24 builds on top of standard No. 19 and prescribes the sealing of the votes cast, thus ensuring its confidentiality. Interestingly, the wording of this provision is aimed at preventing the publication of intermediary results, and is not an end in itself. In this regard, the Explanatory Memorandum states that standard No. 24 "aims at preventing the establishing and publication of intermediary results of the e-voting channel" (Council of Europe 2017b: para. 75).

Nevertheless, secret suffrage should be considered and end in itself and not just a means to prevent the publication of intermediate election results. In fact, a ban on the publication of intermediary results seems more geared towards respecting the principle of equal than secret suffrage (since knowing intermediary results would give advantage to later voters over those who have cast their vote earlier). For this reason, and even if the provision in standard No. 24 is accurate, I think that the aim has been misplaced: if its goal is different from ensuring the voter's "right to vote secretly as an individual" (Council of Europe 2017b: para. 14), then it is not aimed at fulfilling the principle of secret suffrage and should be also moved from this section. This would require, in turn, to come up with a new standard on the need to preserve the voters' choices confidentially.

4.2 The Need for a New Approach

Even more concerning that the flawed scope of these provisions is the fact that the Recommendation has also failed at fully mainstreaming its new approach towards e-voting. In this regard, and in spite of the new benchmark being that "e-voting must respect all principles of democratic elections and referendums" (Council of Europe 2017a: para. i), there are many provisions that are still based on analogies to paper-based voting channel.

This constraint becomes self-evident in the (in)direct references to secret suffrage in the Recommendation. For example, the guidelines for the implementation of standard No 40 read that "[f]rom the moment the vote is cast, no one should be able to read or change it or relate the vote to the voter who cast it. This is achieved by the process of sealing the ballot box, and where the ballot box is remote from the voter, by sealing the vote throughout its transmission from voter to ballot box. In some circumstances, sealing has to be done by encryption.

To seal any ballot box, physical and organisational measures are needed. These may include physically locking the box, and ensuring more than one person guards it. In the case of an electronic ballot box, additional measures are necessary, such as access controls, authorisation structures and firewalls.

A vote is sealed when its content has been subject to the measures that ensure that it cannot be read, changed or related to the voter who cast it" [emphasis added] (Council of Europe 2017c).

These provisions basically translate the processes for the counting of the votes cast on paper to (remote) e-voting. First, they claim that votes are anonymous from the moment they are cast, whereas elsewhere the Recommendation itself mentions that anonymity should be guaranteed before the counting stage (see for example standards No. 26 and No. 45). As a matter of fact, this provision mixes anonymity (not being able to relate a vote to the voter who has cast it) with confidentiality (being able to read the vote). Sealing as described in the Guidelines may ensure confidentiality, but not anonymity. Additionally, the Guidelines prescribe specific measures for the "sealing" of the electronic ballot box, which are "additional" to those used for physical ballot boxes. It is unclear whether the same measures can be applied at all, or whether the Recommendation should have prescribed equivalent measures. Lastly, these provisions use vague wordings such as "sealing", which does not mean anything specifically.

Therefore, an alternative approach would be to actually derive the standards from the different dimensions of secret suffrage (Rodríguez-Pérez 2021: 382). Also based on the Venice Commission's Code of Good Practice in Electoral Matters (2002), the Parliamentary Assembly of the Council of Europe (PACE) has identified three main standards in secret suffrage (2007: 5–6):

- Individuality, meaning that each voter makes an individual choice.
- Confidentiality, meaning that only the voter should know how they have voted, and they should be able to make their choices in private.
- Anonymity, meaning that there should not be a link between the vote cast and the identity of the voter who has cast it.

In what follows, I discuss if the current provisions in the Recommendation clearly address these three standards and how they do it.

About Confidentiality in i-voting. Confidentiality is possibly the standards that has been more accurately addressed in Rec(2017)5. In this regard, standard No. 19 enshrines the standard of confidentiality, broadly understood as "the secrecy of the vote" (Council of Europe 2017a). The reference to "encryption" (Council of Europe 2017b: 41) in the Explanatory Memorandum is in this regard paramount, since most of the systems used nowadays ensure the confidentiality of the votes cast with end-to-end encryption. More importantly, standard No. 25 identifies the need to preserve the confidentiality of previous choices, something that is quite unique to (remote) e-voting.

Standard No. 24 could be linked to confidentiality as well, since it calls for preventing the number of votes cast for each option from being known. However, I have already mentioned that the goal of this standard should be confidentiality *as such*, and not to prevent "the establishing and publication of intermediary results of the e-voting channel" (Council of Europe 2017b: para. 75).

However, the main concern regarding the standard of confidentiality is that there are no specific provisions for long-term privacy. In fact, standard No. 19 is meant to apply "throughout the entire procedure: in the pre-voting stage (e.g. transmitting of PINs, or electronic tokens to voters), during the completion of the ballot paper, the casting and transmission of the ballot and during counting and any recounting of the votes" (Council of Europe 2017b: para. 63). Only he Guidelines on Standard No. 40 point briefly towards post-election data processing, by specifying that "[a]ny data retained after the election or referendum period should be stored securely" (Council of Europe 2017c: 40m). Therefore, it is not clear what may happen with the votes after an election is over.

In this regard, it should be noted that current encryption schemes will be vulnerable against quantum computing. In 1994, Peter Shor found an algorithm that could be implemented by a quantum computer to break contemporary encryption algorithms (Hoofnagle and Garfinkel 2022: 166–167). Regardless of when quantum computers may be available to break these algorithms, any data that is published today is vulnerable against future quantum attacks. According to Ward Beullens et al., “[w]hat makes matters worse is that any encrypted communication intercepted today can be decrypted by the attacker as soon as he [sic] has access to a large quantum computer, whether in 5, 10 or 20 years from now” (2021: 28). In my opinion, the Council of Europe’s Recommendation could provide some guidance on how to deal with this challenge (or at least envisage that the confidentiality of the data should be ensured also after the election).

About Anonymity in i-voting. Anonymity is also dealt with in Rec(2017)5. Standards No. 19 and No. 26 are the main provisions. Standard No. 26 reads that “[t]he e-voting process, in particular the counting stage, shall be organized in such a way that it is not possible to reconstruct a link between the unsealed vote and the voter” (Council of Europe 2017a: 6). Therefore, the Recommendation already acknowledges that some link may be kept, as it is often the case for i-voting (Council of Europe 2017b: para. 79): until the counting stage, the encrypted vote (sealed in postal voting) is kept to together with some voter identifier to ascertain that all votes have been cast by eligible voters and to ensure that only one vote per votes is counted and included in the final tally. The wording of this provision thus acknowledges that, in contrast to what tends to happen with paper-based voting in polling stations, remote voting channels (be them electronic or not) always tend to link the identity of the voter to the sealed vote. In this regard, the stress that the link cannot be established with the “unsealed vote” does show that there have been some advances in breaking with the analogies.

The problem with anonymity is how the counting processes is described throughout the Recommendation. Therefore, and in spite of the above-mentioned provisions focusing on what should not happen to ensure anonymity (i.e., not having a link with the unsealed vote), Rec(2017) resorts to analogies when describing the steps in the counting procedures. The best example are the provisions in the Explanatory Memorandum for standard No. 26: it prescribes that “[t]he separation [of the information linked to the voter and the votes] has to be made electronically at a predefined stage before counting takes place” (Council of Europe 2017b: para. 79). Moreover, the Explanatory Memorandum for Standard No. 45 draws a straight analogy to paper-based voting channels: “(and by analogy with the physical ballot box), before unsealing, votes are mixed” (Council of Europe 2017b: para. 134).

Interestingly, in a previous provision it has been acknowledged that “[i]n the case of internet voting, there exist encryption methods that do not require decoding before votes are counted (homomorphic encryption). Counting can be performed without disclosing the content of encrypted votes” (Council of Europe 2017b: para. 62). However, the remainder of the Rec(2017)5 and the related documents do not seem to take this possibility into account. In this regard, with homomorphic tallying it is not even necessary to separate the data as prescribed in standards No. 26 and No. 45 at all.

Lastly, it should be considered whether the provisions on secret and equal suffrage could be included as a requirement for anonymity. In this regard, provisions for Standard

No. 6 in the Explanatory Memorandum mention that "[w]hen the number of e-votes or of paper votes is particularly small there is the risk that vote secrecy may be violated if the results of those few votes are disclosed" (Council of Europe 2017b: para. 7). This is not unique to (remote) electronic voting, but electronic means can be seen as more easily ensuring that the number of votes in the result is high enough to prevent anyone from inferring what each voter has voted. For example, the system could have checks preventing the contents of a ballot box from being decrypted if the number of votes it contains is lower than a pre-defined threshold, and automatically aggregate them with the cyphertexts of another ballot box to tally the election results at a higher level.

About Individuality in Remote Electronic Voting. Lastly, individuality is slightly touched upon in Standard No. 23. Standard No. 23 reads that "[a]n e-voting system shall not provide the voter with proof of the content of the vote cast for use by third parties" (Council of Europe 2017a). To ensure individuality in (remote) e-voting, the Explanatory Memorandum identifies some measures, such as "criminal law provisions" (Council of Europe 2017b: para. 71) and informing voters "on the necessity to delete traces of the voting transaction from the device used to cast the vote and on how to do so" (Council of Europe 2017b: para. 73).

This little attention paid to individuality in the Recommendation is quite striking. Specially if one takes into account that one of the main concerns about i-voting is the fact that voters may be forced to vote in a certain way under duress if they vote from uncontrolled environments (Watt 2003; Birch and Watt 2004; Vollan 2006; Enguehard 2010; Buchstein 2015; Manin 2015; Teorell et al. 2016). This concerns have been mitigated in some cases by allowing voters to cancel any vote that they may have cast electronically, either by voting again online or in a polling station. In fact, Estonia and Norway are well-known examples of countries offering such possibility. In contrast, Rec(2017)5 only addresses multiple voting in order to acknowledge this practice. For example, the guidelines on Standard No. 9 prescribe that "[i]f a voter is allowed to cast an electronic vote multiple times, appropriate measures should be taken to ensure that only one vote is counted" (Council of Europe 2017c).

Whereas the Recommendation may not be the right instrument to impose an obligation on states to adopt multiple voting in i-voting, it should at least address this issue more carefully. At the end of the day, the definition of secret suffrage in the Recommendation also sets that "the state has the duty to protect that right [to vote secretly]" (Council of Europe 2017b: para. 14). Notwithstanding, how the state can protect this right when voters cast their vote electronically from uncontrolled environments remains unaddressed.

4.3 The Need for an Update?

In principle, one of the advantages of the updated Recommendation is its three-tiered structure. The new structure allows for distinguishing between principles, recommendations, standards, and requirements. Principles come from various international legal instruments and not from the Recommendation as such. Recommendations are contained in the Recommendation (paragraphs i. to vi.).

Standards are included in the Appendix I to the Rec(2017)5 (Driza Maurer 2017: 150) and can be distinguished between "legal standards" and "technical standards" (Driza Maurer 2017: 152). Legal standards "set objectives that e-voting shall fulfil to conform to the principles of democratic elections" (Driza Maurer 2017: 152), while technical standards "refer to a technical norm, usually in the form of a formal document that established uniform engineering or technical criteria, methods, processes and practices" (Driza Maurer 2017: 152). According to Ardita Driza Maurer, "the Guidelines [. . .] offer instructions on the implementation of the standards" (2017: 152).

Since they come from different legal sources (principles from international conventions and treaties, national constitutions and formal law; standards from international recommendations and soft-law, and from national material law; and requirements from lower-level regulations), there is in principle a "hierarchy between principles (top), standards (middle) and requirements (bottom of the pyramid)" (Driza Maurer 2017: 152–153).

Another advantage of this layered approach is that it allows for taking stock of rapid technological change. For example, the rationale for the Guidelines is that "they are supposed to evolve frequently to take stock of legal and technical developments" (Driza Maurer 2017: 154). Furthermore, the Recommendation also introduces "a review policy for the Recommendation which is based on the previous practice of biannual meetings" (Driza Maurer 2017: 154). According to Ardita Driza Maurer, these meetings could be used to consider the update of the Guidelines (2017: 154).

Taking into account this new structure, is it possible to identify (at least) three potential future scenarios for the provisions on secret suffrage in Rec(2017)5:

1. Rec(2017)5 is updated to address these flaws. A complete review of the Recommendation, the Explanatory Memorandum, and the Guidelines would allow for moving the provisions on data protection outside the scope of secret suffrage, review the aim of some standards, and accurately assess the wording of all the provisions related to this principle. In this scenario, the assessment should not be limited to secret suffrage: it may be necessary to address potential flaws regarding the provisions on universal, equal, and free suffrage, as well as on the regulatory and organisational requirements, on transparency and observation, etc. Whereas this is the ideal scenario, it is unlikely to happen given that the Recommendation was reviewed just five years ago and that prior shortcomings did not trigger an immediate update either.
2. Rec(2017)5 remains as it is, regardless of its flaws. The alternative is the *status quo*: the Recommendation remains as it is, including with these inconsistencies. This seems unfortunately the most likely scenario, given the fact that the Recommendation's review policy seems to have shifted towards other technologies in the electoral cycle (Council of Europe 2022), rather than providing an actual review mechanism for Rec(2017)5. Since the Recommendation is a voluntary soft-law standard, it is likely that states following this guidance manage to overcome any of Rec(2017)5's flaws when translating the standards into their national legislation.
3. Specific guidelines are adopted on the implementation of Rec(2017)5. A third alternative exists that takes advantage of Rec(2017)5's new review policy. In this scenario, the Recommendation remains as it is, but the Guidelines are reviewed. This seems feasible, but the problem is that the main shortcomings that I have identified

can be found in the Recommendation itself and in the Explanatory Memorandum, which would not be changed. To compensate these shortcomings, the development of specific Guidelines on secret suffrage and remote e-voting could be considered. These Guidelines could develop the provisions in the Recommendation and recognize some of its limitations. Since the provisions on data protection would remain under the umbrella on secret suffrage, specific Guidelines on personal data protection and remote e-voting could be developed as well. This would provide a platform to clarify the scope of personal data protection as being broader than secret suffrage and to identifying and develop the main principles for personal data protection in European data protection law for (remote) e-voting.

5 Conclusions

Provisions on secret suffrage are dispersed throughout Rec(2017)5 and its related documents. The main provisions can be found in Section of Appendix I. IV, but the principle is also mentioned directly or indirectly in several other sections. A detailed analysis of these provisions reveals important flaws in the understanding of secret suffrage in (remote) e-voting. Some of the flaws are the result of an inaccurate understanding of secret suffrage, in which this principle is mixed with provisions on personal data protection. In a similar way, some of the provisions also point towards secret suffrage being a means to achieve other principles, rather than an end on itself. In other cases, the flaws are due to analogies being drawn with paper-based voting channels, which prevent the standards from taking stock of the specificities of (remote) e-voting.

The paper advances potential future scenarios for Rec(2017)5. Among the three potential scenarios, a full update is the more desirable: it is the only option that would allow for rescoping the provisions on secret suffrage, moving the provisions on personal data protection to another section and addressing some of the definitions for the standards in Section IV. However, this alternative is very unlikely. Therefore, and since the current situation could be improved, a better alternative would be to adopt new Guidelines for Rec(2017)5. One set of guidelines would develop the provisions on secret suffrage, identify the three standards in this principle (individuality, confidentiality, and anonymity), and recognize some of the current shortcomings in the Recommendation and the Explanatory Memorandum. A second set could be adopted on personal data protection: to clarify the scope of personal data protection as being broader than secret suffrage and to identifying and develop the main principles for personal data protection in European data protection law for (remote) e-voting.

References

Barrat i Esteve, J., Goldsmith, B.: Compliance with International Standards. Norwegian E-Vote Project. Washington, United States: International Foundation for Electoral Systems (2012)

Beullens, W., et al.: Post-Quantum Cryptography: Current state and quantum mitigation. European Union Agency for Cybersecurity (ENISA) (2021)

Birch, S., Watt, B.: Remote electronic voting: free, fair and secret? Polit. Q. Publishing **75**(1), 60–72 (2004)

Buchstein, H.: Public voting and political modernization. Different views from the nineteenth century and new ideas to modernize voting procedures. In: Elster, J. (ed.) Secrecy and Publicity in Votes and Debates, pp. 15–51. Cambridge University Press, New York (2015)

Council of Europe: Recommendation Rec(2004a)11 of the Committee of Ministers to member states on legal, operational and technical standards for e-voting (2004a)

Council of Europe: Explanatory memorandum to the Recommendation Rec(2004b)11 of the Committee of Ministers to member states on legal, operational and technical standards for e-voting (2004b)

Council of Europe: Guidelines on transparency of e-enabled elections (2010a)

Council of Europe: Certification of e-voting systems: Guidelines for developing processes that confirm compliance with prescribed requirements and standards (2010b)

Council of Europe: Recommendation CM/Rec(2017a)5 of the Committee of Ministers to member States on standards for e-voting (2017a)

Council of Europe: Explanatory Memorandum to Recommendation CM/Rec(2017b)5 of the Committee of Ministers to member States on standards for e-voting (2017b)

Council of Europe: Guidelines on the implementation of the provisions of Recommendation CM/Rec(2017c)5 on standards for e-voting (2017c)

Council of Europe: Committee of Ministers' Guidelines on the use of information and communication technology (ICT) in electoral processes in Council of Europe member States (2022)

Driza Maurer, A.: Ten years Council of Europe Rec(2004)11. Lessons learned and outlook. In: Krimmer, R., Volkamer, M. (eds.) Proceedings of Electronic Voting 2014 (EVOTE2014), pp. 111–117. TUT Press, Tallinn (2014)

Driza Maurer, A.: Report on the Scope and Format of the Update of Rec(2004)11, Council of Europe (2015)

Driza Maurer, A.: Updated European standards for e-voting. In: Krimmer, R., et al. (eds.) Electronic Voting. E-Vote-ID 2017. Lecture Notes in Computer Science, vol. 10615, pp. 127–145. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-68687-5_9

Ehringfeld, A., Naber, L., Grechenig, T., Krimmer, R., Traxl, M., Fischer, G.: Analysis of Recommendation Rec(2004)11 based on the experiences of specific attacks against the first legally binding implementation of e-voting in Austria. In: Krimmer, R., Grimm, R. (eds.) Electronic Voting 2010 (EVOTE10). Lecture Notes in Informatics (LNI) - Proceedings Series of the Gesellschaft für Informatik (GI), vol. p-167, pp. 225–237 (2010)

Enguehard, C.: Introduction à l'analyse de chimères technologiques, le cas du vote électronique. Cahiers Droit Sci. Technol. **3**, 261–280 (2010)

Essex, A., Goodman, N.: Protecting electoral integrity in the digital age: developing E-voting regulations in Canada. Election Law J. **19**(2), 162–179 (2020)

European Commission for Democracy Through Law (Venice Commission): Code of Good Practice in Electoral Matters: Guidelines and Explanatory Report. Adopted by the Venice Commission at its 51st and 52nd sessions (Venice, 5–6 July and 18–19 October 2002)

Hoofnagle, C.J., Garfinkel, S.: Law and Policy for the Quantum Age. Cambridge University Press, Cambridge (2022)

Jones, D.: The European 2004 draft e-voting standard: some critical comments (2004). http://homepage.cs.uiowa.edu/~jones/voting/coe2004.shtml

Manin, B.: Why open voting in general elections is undesirable. In: Elster, J. (ed.) Secrecy and Publicity in Votes and Debates, pp. 209–214. Cambridge University Press, New York (2015)

McGaley, M., Gibson, J.P.: A critical analysis of the Council of Europe recommendations on e-voting (2006). https://www.usenix.org/legacy/event/evt06/tech/full_papers/mcgaley/mcgaley.pdf

Parliamentary Assembly of the Council of Europe: Secret ballot – European code of conduct on secret balloting, including guidelines for politicians, observers and voters. Resolution 1590 and Report (2007)

Rodríguez-Pérez, A.: My vote, My (Personal) data: remote electronic voting and the general data protection regulation. In: Krimmer, R., Volkamer, M., Beckert, B., Küsters, R., Kulyk, O., Duenas-Cid, D., Solvak, M. (eds.) E-Vote-ID 2020. LNCS, vol. 12455, pp. 167–182. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-60347-2_11

Rodríguez-Pérez, A.:Regulating internet voting by analogy: does it work? Challenges and concerns for secret suffrage. Krimmer, R. et al. (eds.) Sixth International Joint Conference on Electronic Voting E-Vote-ID 2021, 5–8 October 2021, University of Tartu, pp. 381–382 (2021)

Stein, R., Wenda, G.: The Council of Europe and e-voting: history and impact of Rec(2004)11. In: Krimmer, R., Volkamer, M. (eds.) Proceedings of Electronic Voting 2014 (EVOTE2014), pp. 105–110. Tallinn, TUT Press (2014)

Swiss Federal Chancellery: Modification de la loi fédérale sur les droits politiques (Passage de la phase d'essai à la mise en exploitation du vote électronique). Rapport explicatif pour la procédure de consultation (2018)

Swiss Federal Council: Évaluation de la mise en place du vote électronique (2006–2012) et bases de développement (2013)

Teorell, J., Ziblatt, D., Lehoucq, F.: An introduction to special issue: the causes and consequences of secret ballot reform. Comp. Polit. Stud. **50**(5), 531–554 (2016)

Vollan, K.: Voting in uncontrolled environment and the secrecy of the vote. In: Krimmer, R. (ed.) Electronic Voting 2006 – 2nd International Workshop, Council of Europe, ESF TED, IFIP WG 8.6 and E-Voting, CCpp. 155–169 (2006)

Watt, B.: Human rights and remote voting by electronic means. Representation **39**(3), 197–208 (2003)