ied Institute of European Democrats

THE FUTURE OF DEMOCRACY IN THE EUROPEAN CONTEXT

THE FUTURE OF VOTING
HOW ICT IMPACTS VOTING AND WHAT TO DO ABOUT IT?

Author: Ardita Driza MAURER

Brussels, February 2022

Rue Montoyer 25
1000 Brussels
Belgium

Web: www.iedonline.eu

This Research Paper was elaborated on the basis of independent research. The opinions expressed here are those of the Contractor and do not represent the point of view of the Institute of European Democrats.

With the financial support of the European Parliament

EXECUTIVE SUMMARY

Democracy and elections, like any other field, have seen a steady increase in the use of information and communication technologies (ICT) in the past 20 years. The development and use of ICT solutions in elections should obey to the principles of democratic and free elections, namely universal, equal, free, secret and direct suffrage. Making sure that this is the case implies several steps that will be analysed in this paper.

Social Media summary

How can we approach the possible digital future of voting to make sure that it will comply with the principles of free and democratic elections ?

Keywords

#ICTinelections, #evoting, #ecounting, #eregisters, #electoralprinciples, #constitutionalconformity

Short bio

Ardita Driza MAURER is an independent legal consultant. She contributes as lead expert to the Council of Europe *Guidelines on the use of ICT in electoral processes,* approved by the European Committee on Democracy and Governance (CDDG) on 29 November 2021 and expected to be approved by the Committee of Ministers. She was lead expert for the Committee of Ministers *Recommendation Rec(2017)5 on standards for e-voting* and related *Guidelines*. The Council of Europe has done pioneering work, being the only international organisation to have issued guidance to the attention of member States on regulating of use of ICT solutions in elections.

Contents

1. **Introduction**

Democracy and elections, like any other field, have seen a steady increase in the use of information and communication technologies (ICT) in the past 20 years. ICT-backed solutions are now used throughout the voting processes. Most voting-related data exist in digital only or in digital and paper formats. Flagship projects, like e- voting, have experienced ups and downs and are little used today in Europe, although, in the COVID19 context, discussion about their use has resumed. Other ICT solutions, less visible, but important for the overall conduct of voting (e.g. e-solutions for handling registration, election information, polling day activities, results, etc.), have quietly made their way into the electoral processes of all countries in the Council of Europe region and beyond.

We discuss here, in general, the use of ICT solutions used during the different steps of a voting process: from voter and candidate registration, to other preparatory steps, to voting itself, counting, control of results, etc. One important step – campaigning – is excluded, because use of ICT (keyword: social media) for campaigning and opinion-formation purposes is a much broader area of ICT influence on elections, involving many different actors. We limit our considerations to those uses of ICT in elections whose introduction, control, development or abandonment is exclusively in the competence of the state electoral authorities, be it the executive, the legislator, or other lower administrative units.

It is understood that ICT (and all other) solutions used in elections should obey to the principles of democratic and free elections, namely universal, equal, free, secret and direct suffrage, and the conditions for implementing them[1] as well as to any other relevant constitutional principle. However, this has proved easier to uphold in theory than it is to implement and measure in practice. In this short paper we focus on issues related to the constitutional conformity of ICT solutions used in the voting process.

Recent elections in established democracies, namely the two last US Presidential elections, have shown that it is not just social media activities that greatly impact elections. ICT-backed "small" solutions, employed by local or central authorities to support registration, voting and counting, can become targets and entry-points for attackers who seek to exert illegal influence over an election process, namely state actors. Even if the inherent vulnerabilities of such solutions are not exploited, their existence raises and maintains suspicions about the integrity of the process.

If vulnerabilities are exploited, attackers may suppress or change legitimate data, introduce illegitimate one, cause confusion, delays and other disruptions during the process and overturn the outcome. The realization of the electoral principles will be compromised, and the outcome will not reflect universal, equal, free, secret or direct suffrage. Ultimately this will affect trust in elections. It is thus important to make wellthought, balanced decisions on the development and use of ICT in voting processes, considering both the hoped for benefits (e.g. on efficiency,

[1] Also known as the *European Electoral Heritage*, these principles are shared by all Council of Europe countries. They are referenced in the European Commission for Democracy through Law (Venice Commission) *Code of Good Practice in Electoral Matters*, 2002. Available at https://rm.coe.int/090000168092af01

accessibility, suppress human error, etc.) and the risks that come with ICT and threaten the confidentiality and integrity of the data and of the outcome. As voting processes developed gradually over the past two centuries around paper/low-tech solutions, it is important, when envisaging a possible digital future for them, to understand the implications of introducing ICT. ICT-backed solutions bring paradigm changes to the organization of voting which need to be regulated and handled properly. If not, ICT may compromise the respect of electoral rights and the constitutional conformity of the process.

In order to ensure that ICT solutions respect electoral principles, it is important to start by considering at least two preliminary questions. First, the authorities should be clear about the values and principles that underpin the process and the role that legal principles should play in framing and orienting the development of e-solutions. Second, it is necessary to understand how the use of ICT impacts legal conformity of the voting processes. We look at these two aspects in the following paragraphs and conclude with a few recommendations to the attention of policy makers on how to approach the possible digital future of voting to make sure that it will comply with the principles of free and democratic elections. Recommendations are based on academic research and countries' experiences.

2. The guiding role of electoral principles

2. 1 Rights *vs* Techniques for expressing rights

It is often said that ICT introduces new democratic participation forms so, it is *de facto* welcomed. It is not clear however what kind of participation or which ICT this refers to exactly. In practice, several countries have introduced solutions like e- collecting or e-voting to enable newly introduced rights like launching initiatives and referenda and voting on such issues. New referendum rights and new e-solutions (e-voting, e-collecting) that enable them are introduced or planned to be introduced in Iceland, Croatia, Lithuania or Denmark, however, e-voting in these cases is only al- lowed for referendums. Elsewhere (e.g. in France), e-voting is part of the ongoing debate about the development of direct democracy options.

The simultaneous introduction of new participatory rights and new e-solutions may suggest that the two go automatically together so that new participation forms require necessarily the introduction of ICT-backed solutions. This is simply not true, as we explain below. And there are other good reasons for *separating the debate about new rights from the one about the solutions* that enable the expression of rights.

When envisaging the introduction of e-voting or e-counting, it is recommended to start small and proceed progressively.[2] The introduction of new participatory rights is often done gradually as well. So, it can make sense to "couple" these two gradual developments. However, it is erroneous

[2] See the Council of Europe Recommendation CM/Rec (2017)5 on Standards for E-voting. Available at https://www.coe.int/en/web/portal/news-2017/-/asset_publisher/StEVosr24HJ2/content/council-of-europe-adopts-new-recommendation-on-standards-for-e-voting

to infer that without e-voting or e-collecting, it would be impossible to introduce or extend initiative or referendum rights.

New participatory rights influence the repartition of power between the People, the elected legislator and the executive and are usually foreseen in the Constitution. Decisions about their development and extension usually involve the legislator and require dedicated thinking. Furthermore, such rights have been developed and have thrived in several countries (e.g. US States, Switzerland, Italy, etc.) centuries before ICT came to exist. In Switzerland, e-voting was used in a limited way from 2004 to 2019. However, use its use or its current suspension had no impact on the ability of Swiss cantons to hold referendums and initiatives. While *e-voting* and *e-collecting* may potentially enhance direct democracy rights, they *are not a conditio-sine-qua-non for introducing or developing initiative or referendum rights*.

Introduction of ICT in elections, on the other side, merits to be evaluated on its own considering both the opportunities it offers and the risks it entails. By associating the extension of rights with the introduction of ICT solutions, there is a *risk of introducing a positive bias towards the e-solution*. Sheer enthusiasm about ICT, if not balanced by a clear understanding and discussion of risks as well as an appropriate risks' management policy, may eventually violate or discredit the very participation rights that it seeks to promote.

2.2 Identifying the best solution

It often goes like this: "ICT is introduced because it brings added value compared to low-tech solutions". The advantages of ICT, compared to manual procedures, in terms of efficiency and correctness (i.e. elimination of unintended human error) seem clear. And ICT-solutions may be tailored to offer better access to people with special needs, like the blind or the sight-impaired. These advantages, however, do not mean that ICT is *always* advantageous. The capacity of ICT solutions to implement and comply with electoral rights should be in the spotlight. At the end, ICT is one possible technology among others.

The best approach is to *start by considering the problem that needs to be solved* or the improvement to be achieved. Then, one should identify all possible solutions (paper, low-tech, ICT ones, etc.) and compare their advantages and disadvantages. Finally, the most appropriate one can be chosen, taking into account the context, namely the process into which the envisaged solution will be integrated. Such context may still be dominated by paper-based manual procedures, and an adapted solution can also consist in a mixture of paper and ICT.

It is important to look for the best solution in the context and not for a best solution in absolute terms, which could be impracticable in the given context. Unfortunately, too often, it's the for-profit vendors who initiate developments in this field, by putting pressure to sell their solutions. Instead of considering the problem and the needs, work starts with a clear ICT solution in mind: the one proposed by the vendor. And, quite often, decision makers seem to assume that ICT solutions are anyway superior to low-tech ones.

The search for new or better solutions should come from those in charge of organizing and supervising the voting processes and should aim at addressing the needs and expectations of those affected by the problem or interested in improving the solution. For instance, if the hoped-for improvement is the efficiency of the counting process, one should get, first, a clear view of the existing situation and of the issues that affect counting efficiency. In other words, new solutions introduced in the voting process should be *needs-driven and not vendor-driven*.

Identifying the initial problem that needs to be addressed helps also to distinguish it from problems that will be introduced by … the solution. No technology and ICT no solution can satisfy completely and simultaneously all electoral principles. Principles of free and democratic elections include competing rights: secrecy competes with controls necessary to ensure free suffrage; universal and equal access may compete with secret and free suffrage, etc. So, *the best solution always relies on a good balance between competing rights*. A new solution will solve certain problems while introducing others. To explain why, on balance, the new solution is the best option, it is important to remind the initial situation and the different options available for solving the identified problem.

2.3 Electoral principles to frame and guide ICT

It is often stated that high-level electoral principles should frame and guide the development of ICT solutions for elections. The practical implementation of it, however, is quite a challenge. The statement can be broken down into at least four parts: first, we know the principles; second, the principles should guide the development of an ICT solution; third, an ICT solution should implement and respect the principles; and fourth, it follows that legal principles prevail over ICT solutions.

To *know the principles* means to identify all relevant principles and derived requirements that a solution must respect. In addition to the international core principles of the European electoral heritage identified by Venice Commission, relevant national and also local ones apply. Next, one must decide what is the minimum level of application for each involved principle.

As already mentioned, electoral principles include competing values. It is impossible, for any solution, be it ICT or paper-based, to respect simultaneously all principles in their entirety. So, one must decide what is the minimum level of implementation, the correct balance to be found for competing principles. E.g., if a solution offers advantages in terms of accessibility (universal and equal suffrage) but is more vulnerable to breaches of secrecy or of integrity (free and secret suffrage), what is the minimum level of each principle to be ensured in the specific context in which it will be used (if used only by a limited group such as the sight impaired, tolerance to the mentioned risks may be higher, than if the solution is used by the whole electorate).

Discussions about the minimum level of implementation of principles are of legal and political nature and require the involvement of the legislator. Legal decisions should frame and limit the discretion of the executive / IT experts that develop and implement e-solutions. This is how *legal principles guide the development of ICT*. Unlike paper-based, manual processes, ICT solutions are mathematical constructions which require that all conditions are spelled out clearly and exhaustively before designing the solution.

A detailed legal regulation, which includes decisions on the minimum level of implementation of competing principles, is required before the solution is developed. Such decisions cannot be left to the discretion of IT experts or even less to interpretations and adjustments during implementation. The "translation" of legal principles into legal and technical requirements requires competent and combined expertise, from the legal and technical fields.

The next step towards a *compliant ICT solution* is to have it evaluated, by a competent body, and found to respect the principles (e.g. *certification process*). Respect for the principles should also be ensured during the actual operation of the ICT solution. Different checks (e.g. *audits*) are introduced for this purpose. No ICT system in the world can offer perfect security and there exists no realistic mechanism able to fully secure computer systems used for vote casting and tabulation of results from cyber threats.[3] A *risk management framework* should periodically evaluate threats, vulnerabilities and ensuing risks and decide on their acceptability and how to handle them. An ICT solution can be secured against certain risks, however there will always be *remaining risks*. Predefined rules to deal with them are important. In addition, it is important to identify and discuss the *underlying assumptions* of the security concept (see discussion of assumptions below).

To conclude, ensuring that ICT complies with the principles involves, first, a number of decisions of principle about opportunities and risks, evaluation and verification options, remaining risks, assumptions and a risk management framework, among others, which have an important legal and political dimension. The active involvement of the legislator and regulator is paramount.

Stating that *legal principles prevail over ICT solutions* means to recognise that the work of interpreting the principles and deriving legal and technical requirements should precede and guide the development of the ICT solution. Indeed, the solution should be (built) based on such requirements. In practice however, quite often, an important part of the legal work is done after a solution is developed. Efforts are then put into "adapting" the legal requirements to the existing solution instead of doing just the opposite. This should change. It is important that the legal regulator has a good understanding of the legal questions that ICT raises and it is crucial that the legal principles and values remain the leading force that determines the development of ICT solutions used for elections.

3. The impact of ICT on the realization of electoral principles

Use of ICT solutions challenges the realization of electoral principles during voting processes. Why and how? To illustrate the paradigm changes introduced by ICT, let us look at examples of how ICT affects security and trust in elections. These two aspects are important for all solutions used in voting processes. Such changes need to be understood and addressed at the regulatory level.

[3] National Academies of Sciences, Engineering, and Medicine. 2018. *Securing the Vote: Protecting American Democracy*. Washington, DC: The National Academies Press. https://doi.org/10.17226/25120

3.1 Use of ICT impacts election security

An *election should be secure and perceived to be secure*. Security is the guarantee that all relevant rights and obligations are upheld throughout the process. The State has the positive obligation to ensure security of elections, including of ICT-backed solutions used in the voting process. In practice, ICT challenges the way election security is organised so far. Below are a few illustrative examples: traditional checks are meaningless and new checks need to be developed; security must rely on convincing evidence which consists in mathematical proofs; these are not understood by the layman; users are however meant to play an active role in securing the system, by performing checks; usable security is an important research topic. Security of ICT in elections is, in general, a broad research field.

Errors are unavoidable in paper-based voting processes, given that failure is inherent to manual operations. In addition, there is the risk of illegal manipulation. However, paper-based voting and counting operations can be *checked by examining the paper trail* (registers, ballots, counting minutes, etc.). If well-conserved, paper trail offers the guarantee that errors and manipulations can be detected. The other advantage is that such controls can be conducted and overseen by laypersons, without specialized technical knowledge, to make sure that outcomes are correct. Finally, paper- based operations being usually done at polling stations level, successful attacks in any of them will have an impact limited to the specific polling stations. It is important to have adequate procedures that enable detection and, if possible, correction of any irregularity. Given these, the system can be considered secure.

ICT backed solutions do solve the issue of human error as it is usually impossible to make unintended errors by following the ICT procedures. However, ICT comes with inherent new vulnerabilities. It is exposed to cyberthreats coming from internal and external malicious actors which need to be dealt in a risk management framework. Beyond this, use of ICT involves complex checks and proofs which question the involvement of laypersons and of the electorate in ensuring public control of the outcome. Some ICT solutions include paper records in parallel to e-records. These are easier to control, similar to the above-mentioned paper-based controls. Most other ICT solutions though, exclude paper. In these cases, keeping paper records in parallel to e-records is simply meaningless. For instance, paper prints of internet votes make no sense as they will be potentially as corrupted as their electronic version. So, other types of *controls* need to be introduced to verify the integrity of electronic records, i.e. *to detect possible irregularities in the outcome*.

One main difficulty of checking the outcome of e-solutions in the voting context (as compared for instance to e-banking) stems from the requirement of both transparency and secrecy: voting requires evidence that the result is correct and, at the same time, evidence that the privacy of participation and secrecy of votes is respected. These are conflicting principles.[4] In practice, *cryptographic solutions* are the only known way to implement such conflicting values

[4] For a detailed discussion, see Bernhard *et al.*, “Public evidence from secret ballots” in Krimmer *et al.*, (Eds): E-Vote-ID 2017, pp. 121-140, 2017. Available at https://www.e-vote-id.org/wp-content/uploads/2017/10/TUTPress-2017.pdf

simultaneously and are used in e- voting. Evaluating their security requires complex *mathematical proofs*.

Another aspect of ICT is that the impossibility to fully secure e-solutions (including cryptographic ones), has led research to develop approaches like software independence, end-to-end verifiability, statistical risk limiting audits (RLAs), evidence-based elections, etc. The bottom line is that *ICT solutions cannot be fully secured*, so security must rely on convincing evidence that the outcome is correct. Convincing evidence in this case means, again, mathematical proofs.

Furthermore, *no solution can be considered as being optimal for all kind of election*, so that choosing the right solution is always the result of balancing advantages and disadvantages, analyzing and handling risk and deciding on the acceptability of remaining risks *in* the specific election context. Which means that there is not one-and-for-all valid check of the security of the ICT solution. Such checks should be renewed for each specific use and over time.

Security of ICT solutions questions the role of the public control over the outcome. On the one side, laypersons and even IT specialists are *unable to understand the mathematical proofs* in question (only a very tiny group of specialists may be able to do so, and only for parts of it). On the other side, users, i.e. laypersons, are meant to be active players of the security. Indeed, ICT systems that integrate mechanisms which produce convincing evidence about the outcome, must be *usable by regular voters*, observers, etc. The probability that such mechanisms will effectively detect problems depends on their actual use. It is no longer the State who, alone, must ensure the security of the system. The user, the voter, becomes an important actor of the security. Whether the random user is able to fulfil the role that is assigned to them by the system is still an open research question. Achieving it will require a lot of learning.

So, to sum it up, security of ICT solutions relies first on the participation of laypersons – whose aptitude to assume such role is questionable. Second, security relies on evidence, i.e. mathematical proofs, which can only be understood by a very very small group of specialists. These questions, namely usable security, require *further research*. An initial answer from current research is that when verification relies on experts, layvoters should have the possibility to choose the trusted expert (see discussion on trust below).

As briefly mentioned above, an important aspect of security and, hence, of compliance of ICT with the principles, are assumptions. Security of computer-based solutions relies on several *assumptions*. It is for instance assumed that the user will behave in a certain way, or that the attacker will have only certain capabilities but not others. If assumptions hold, then security is ensured. If any of the underlying assumptions does not hold, then security is compromised, and the principles potentially violated. For an assumption to hold in practice, it should be realistic. Whether an assumption is realistic or not needs to be decided beforehand. Furthermore, assumptions should be reevaluated on an ongoing basis, as part of the regular risk assessment. It is thus crucial to *disclose and discuss the security assumptions of ICT-backed solutions*. However, in practice, this is not the case.

Security assumptions of paper-based processes are not discussed either, however this is not prejudicial if there exist good procedures to detect and correct irregularities. Things are different with e-solutions. Assumptions, in this case, need to be discussed and decided beforehand and become part of the security properties of the e-solution. In practice, vendors are eager to claim that their solution is secure but remain silent about the underlying assumptions. Election authorities, on the other hand, have a vested interest in confirming the regularity of the election, but usually lack the knowledge and capacities to deal with complex crypto graphic/IT issues like the evaluation of assumptions.[5] It is thus even more important that these issues are addressed and decided already in the legislation/regulation.

3.2 Use of ICT affects trust in elections

ICT brings several paradigm changes also with respect to trust in elections. In traditional voting procedures, trust in the election authorities, in the security measures or in the organisation of observation are important criteria. When ICT solutions are used, one should take the other viewpoint: *e-solutions and officials/others handling them should not be considered trustworthy*. Elections and their outcome should be evidence-based, i.e. any observer should be able to verify the reported results based on trustworthy evidence produced by the system itself. Does this eliminate the need to trust? We don't think so. Use of mathematical proofs does not eliminate the need to trust. It just displaces it from the previously trusted actors (authorities, organisational measures, observers, etc.) to new ones (experts). Elections and votes produce social choices whose acceptance is based on public's trust in the outcome of the process. Whether displacing trust from previous actors to new ones will improve public support for the outcome of elections remains to be seen.

As the layperson cannot understand mathematical proofs, he/she should put trust in some experts who can check such proofs. According to research, laypersons should be *free to choose the trusted expert*. Which raises the question of choice because, as mentioned, eligible experts are a very tiny part of the IT community. Furthermore, experts will use some other software and hardware to check the mathematical proofs. So, trust is transferred to these other… e-solutions. Furthermore, what happens if experts (including "alleged" experts) disagree? The issue will need to be decided by the judge – who is a layperson with respect to mathematical proofs. These are complex questions which need to be thoroughly discussed and decided at the legislation/regulatory levels.

The bottom line is that while ICT claims to eliminate the need to trust, it actually only displaces it towards mathematical proofs, experts and peer-reviewed algorithms. Whether this is enough to implement the requirement of public control, is an open question which has to be answered by each jurisdiction.

For instance it has already been answered differently in a few different countries. The most known and discussed decision is the one by the German constitutional court who, in 2009[6], said that controls should be understandable by the layperson without specific knowledge and without the

[5] For a comprehensive overview of the challenges that the use of ICT in voting poses to election authorities, see a recent paper by German researchers active in e-voting research: Beckert *et al.*, *Aktuelle Entwicklungen im Kontext von Online-Wahlen und digitalin Abstimmungen*, of 10.09.2021, https://publikationen.bibliothek.kit.edu/1000137300

[6] Bundesverfassungsgericht (2009), Decision 2 BvC 3/07, 2 BvC 4/07, of 3 March 2009, http://www.bundesverfassungsgericht.de/entscheidungen/cs20090303_2bvc000307.htm

help of experts. This is a *de facto* ban on the use of certain ICT solutions (like e-voting) in elections.

4. Recommendations

The development and use of ICT solutions in elections should obey to the principles of democratic and free elections, namely universal, equal, free, secret and direct suffrage. Making sure that this is the case implies several steps.[7] A few preliminary questions are important to be considered by decision makers, at least from the perspective of ensuring constitutional compliance of the future solution.

I. What are the rights that the solution is expected to concretize? In the (frequent) case of competing rights, what is the minimum level of mandatory concretization/respect of every right involved? What are, hence, the legal red lines that any e-solution must respect?

II. After identifying the rights that need to be concretized, one must search for all eligible solutions and, then, consider the best option. A lot of factors will determine what is best. ICT is not automatically the best-suited solution.

III. If one opts for an ICT-solution, the next question relates to whether and how higher-level principles guide the development of the solution. This is so whether the solution is already there (and may need adaptations) or whether a new solution is going to be built from scratch. The solution should be legally compliant by design.

IV. Finally, during the actual use of the e-solution, the main question is whether such use is legally compliant. In other words, whether electoral principles are upheld during the actual voting process. Not only should the solution be legally compliant; its actual implementation and use should also uphold the values and principles of democratic elections. What is at stake here is to develop adequate controls able to convince the (skeptical) public that the process and its results are genuine and honest.

The focus should be on the realization of the higher-level principles of free and democratic elections. This requires among others interdisciplinary expertise.[8]

[7] For a thorough discussion of these questions see: A. Driza Maurer, *Digital technologies in elections. Questions, lessons learned, perspectives*, Council of Europe, 2020. Available at: https://edoc.coe.int/en/elections/8156-digital-technologies-in-elections-questions-lessons-learned-perspectives.html

[8] An important interdisciplinary conference dealing with these issues is the yearly International Conference for Electronic Voting E-Vote-ID , traditionally held in Bregenz, Austria, with participants from Europe, North and South America, Australia, etc. More information at: https://e-vote-id.org/

5. References

Beckert *et al.*, *Aktuelle Entwicklungen im Kontext von Online-Wahlen und digitalin Abstimmungen*, of 10.09.2021, https://publikationen.bibliothek.kit.edu/1000137300

Bernhard *et al.*, “Public evidence from secret ballots” in Krimmer *et al.*, (Eds): E-Vote-ID 2017, pp. 121-140, 2017. Available at https://www.e-vote-id.org/wp-content/uploads/2017/10/TUTPress-2017.pdf

Bundesverfassungsgericht (2009), Decision 2 BvC 3/07, 2 BvC 4/07, of 3 March 2009, http://www.bundesverfassungsgericht.de/entscheidungen/cs20090303_2bvc000307.htm

Council of Europe Recommendation CM/Rec (2017)5 on Standards for E-voting. Available at https://www.coe.int/en/web/portal/news-2017/-/asset_publisher/StEVosr24HJ2/content/council-of-europe-adopts-new-recommendation-on-standards-for-e-voting

European Commission for Democracy through Law (Venice Commission) *Code of Good Practice in Electoral Matters*, 2002. Available at https://rm.coe.int/090000168092af01

Maurer, A. Driza, *Digital technologies in elections. Questions, lessons learned, perspectives*, Council of Europe, 2020. Available at: https://edoc.coe.int/en/elections/8156-digital-technologies-in-elections-questions-lessons-learned-perspectives.html

National Academies of Sciences, Engineering, and Medicine. 2018. *Securing the Vote: Protecting American Democracy*. Washington, DC: The National Academies Press. https://doi.org/10.17226/25120