Cuadernos de Derecho Electoral
Número 2 (2024) / 239-254

REGULATING THE USE OF ICT IN ELECTIONS: THE CONTRIBUTION OF THE COUNCIL OF EUROPE

Ardita Driza Maurer[1]

Abstract
Information and communication technology (ICT) solutions are increasingly used to support most processes of the electoral cycle. Their regulation must ensure that constitutional principles, in particular those on free and democratic elections, are upheld. The Council of Europe is the only international organisation to have issued minimum legal standards on the regulation of e-voting and of other ICT used in elections. Standards guide national competent authorities when drafting national regulations.

Key words: Council of Europe, elections, European electoral heritage, free and democratic elections, ICT in elections, e-voting, i-voting, e-counting, regulation, recommendation, guideline.

1 Ardita Driza Maurer is a jurist, based in Switzerland. She works as independent consultant with a focus on legal implications of the use of ICT-backed solutions throughout the electoral cycle. She was the lead expert for the two Council of Europe instruments in this area, namely the Recommendation CM/Rec(2017)51 of the Committee of Ministers to member States on standards for e-voting (Adopted by the Committee of Ministers on 14 June 2017) and the Committee of Ministers' Guidelines on the use of information and communication technology (ICT) in electoral processes in Council of Europe member States (Adopted by the Ministers' Deputies on 9 February 2022). Prior to that, she was director of the Swiss federal Chancellery internet voting project.
E-mail: ardita.driza@sefanet.ch

La regulación del uso de las TIC en las elecciones: la contribución del Consejo de Europa

Resumen

Las soluciones que brindan las tecnologías de la información y la comunicación (TIC) se utilizan cada vez más para apoyar la mayoría de los procesos del ciclo electoral. Su regulación debe garantizar el respeto de los principios constitucionales, en particular los relativos a las elecciones libres y democráticas. El Consejo de Europa es la única organización internacional que ha emitido normas jurídicas mínimas sobre la regulación del voto electrónico y de otras TIC utilizadas en las elecciones. Las normas orientan a las autoridades nacionales competentes a la hora de elaborar las normativas nacionales.

Palabras clave: Consejo de Europa, elecciones, herencia electoral europea, elecciones libres y democráticas, TIC en elecciones, voto electrónico, voto por internet, regulación, recomendación, directriz.

1. Introduction

Solutions based on information and communication technologies (ICT) are increasingly introduced by election management bodies (EMBs) to support processes throughout the electoral cycle in the Council of Europe (CoE) region. *Voting machines* are or were recently used in polling stations in Belgium, Bulgaria, or France; *internet voting* is mainly used in Estonia and, in a much more limited manner, in Switzerland, or Iceland (for certain types of votes such as referenda), or Norway (at the local level). *E-counting* of paper ballots is practiced by several countries, including Hungary (for preliminary results only), Latvia, Malta (local elections), Norway, Switzerland (in some cantons for referenda), the United Kingdom. *ICT-backed solutions supporting other processes* of the electoral cycle (other than voting and counting) are widespread. Information from a questionnaire distributed by the CoE secretariat to member States in 2020-2021 showed that some 75 different types of e-documents and e-processes were employed at some point during the electoral cycle in the 24 member States who responded (half of CoE members). All electoral stakeholders (voters, parties, candidates, election administration staff, observers, media, translators, dispute resolution bodies, etc.) use an ICT solution at some point during elections.[2] ICT-backed processes *before voting day* include e-services offered to electors to find and change their polling station, to check and amend their electoral details, to apply for postal voting, to register for voting abroad; signature collection for parties to stand for election; signature collection for national and local referenda. Registers (of electors, candidates, voters, etc.) are digitized documents. *During voting day*, EMBs make use of electronic journals with all important figures and events, e-poll books, electronic data exchange among polling stations (e.g. to ensure the possibility for voters to vote at any polling station during early voting days), transmission of provisional and/or final voting results from polling stations to centres where they are consolidated, and published, seat allocation software, etc. ICT-backed solutions *after voting day* include solutions for checking manual errors, statistical audit methods for checking the plausibility of results, solutions for registration and publication of data on voter turnout, statistics and information. Several countries have recently deployed election management systems, to coordinate and streamline the different ICT solutions. ICT thus plays an important role throughout the electoral cycle in the CoE region.

ICT may offer several *advantages* such as increased efficiency and speed, help avoiding errors associated with manual work, etc. But it also brings *challenges* and risks: ICTs are complex, impossible to observe by laypersons, subject to rapid change and may open the door to unpredictability and even to attacks against the electoral process. It is important hence for election management bodies (EMBs) to take informed decisions on their use and make sure that elections benefit from the advantages offered by ICT whereas risks are minimized and under control of the EMB. If they decide to experiment or use ICT, the very first question an

2 See section 3.3. in Driza Maureret al (2022).

EMB has to answer is that of regulation. Detailed regulation should implement and respect the principles of free and democratic elections and other applicable principles.

How does a constitutionally compliant regulation look like? Countries have been drafting regulations of e-voting since the beginning of 2000 and, in parallel, upon request of its members, the Council of Europe started drafting guiding instruments based on countries' experiences and good practice. CoE started work on e-voting, adopting a first recommendation on legal, technical and operational standards for e-voting already in 2004; a new recommendation on standards for e-voting replaced the previous one in 2017; in 2022, the CoE adopted the guidelines on compliant use of (other) ICT-backed solutions used in elections.

The *Council of Europe* is an international organisation created in the aftermath of second world war,[3] and the continent's leading human-rights organisation. It has created a common legal space, centred on the European Convention on Human Rights (ECHR) whose ratification is a prerequisite for joining the organisation. The CoE has played an important role in identifying basic standards for elections and in issuing guidance on regulation of ICT in elections. It has done so in the frame of its core mission which is to safeguard and realise democracy, human rights and rule of law principles which are common heritage of its member States (art. 1 of CoE Statute). Principles which are common to the region are also known as the European constitutional heritage. Part of that is the so-called European electoral heritage. The CoE supervises the respect of the principles judicially through the European Court of Human Rights (ECtHR). Furthermore, the CoE adopts recommendations and guidelines on the implementation of the principles, such as the instruments we discuss in this paper (cf. section 3).

The paper is organised as follows. Next, it presents a short introduction on the role of the Council of Europe in protecting the European electoral heritage by identifying and codifying the requirements that derive from the principles of free and democratic elections (section 2). Then we focus on our main topic which is that of CoE's guidance (standards) on compliant regulation of ICT solutions used in electoral processes, including the 2017 Recommendation on standards for e-voting and its accompanying documents, and the 2022 Guidelines on use of ICT in electoral processes.[4] According to the 2017 Recommendation, e-voting is the e-casting and e-counting of votes. All other ICT backed solutions fall under the 2022 Guidelines on use of ICT in elections. The standards provide guidance to national authorities in

3 Founded in 1949, the CoE has 46 member States, including all European countries to the exception of Belarus and Russia. Russia ceased to be a member as from 16 March 2022 following its aggression of Ukraine and thus blatant violation of the Council of Europe Statute (CM/Resolution(2022)2).

4 The *Recommendation CM/Rec(2017)51 of the Committee of Ministers to member States on standards for e-voting* (Adopted by the Committee of Ministers on 14 June 2017) elaborated by the Ad hoc Committee of Experts on Legal, Operational and Technical Standards for e-voting (CAHVE), https://rm.coe.int/0900001680726f6f. The Recommendation is complemented by Guidelines and an Explanatory report. The *Committee of Ministers' Guidelines on the use of information and communication technology (ICT) in electoral processes in Council of Europe member States* (Adopted by the Ministers' Deputies on 9 February 2022), elaborated by the European Committee on Democracy and Governance (CDDG), https://search.coe.int/cm?i=0900001680a575d9.

charge of regulating and supervising the use of e-voting and other ICT-backed solutions for elections. We discuss the standards-setting process and the content of the two instruments (section 3). To conclude, we comment on the concrete impact of CoE standards on member States regulatory framework as well as on their inherent limitations (section 4).

2. European electoral heritage

Elections are notoriously national or local events.[5] However, countries in the Council of Europe (CoE) region and beyond, follow some commonly shared principles of free and democratic elections. Known as the European electoral heritage, this set of principles includes global ones (Art. 21.3 of the Universal Declaration of Human Rights and Art. 25b of the International Covenant on Civil and Political Rights). The European Convention on Human Rights (ECHR), the founding instrument of CoE, foresees in article 3, Additional Protocol to the Convention (P1-3 ECHR) the *Right to free elections* according to which *the High Contracting Parties undertake to hold free elections at reasonable intervals by secret ballot, under conditions which will ensure the free expression of the opinion of the people in the choice of the legislature*. An important specificity of the CoE is the presence of the European Court of Human Rights (ECtHR) which rules on alleged violations of the rights set out in the ECHR, by individuals as well as by states. The ECtHR has developed a rich case-law on elections, but there are no relevant decisions, so far, on the compliant regulation or use of ICT in elections.

The CoE has furthermore developed *guiding instruments*. The European Commission for Democracy through Law, or Venice Commission, has "codified" the detailed requirements that compose the right to free elections in two main documents: the Code of good practice in electoral matters and its equivalent for referendums, as well as in several accompanying documents.[6] Despite the "soft-law" status, the Code of good practice in electoral matters is the reference instrument with respect to the European electoral heritage. To be noted, the shared principles and interpretations included in the Code come from countries' legislations and practice. In other words, the Code consolidates and "codifies" existing and broadly shared national solutions. At the same time, it is used by the countries as a reference when updating national regulations for elections. Furthermore, the ECtHR refers in its decisions to the Codes of good practice, giving them obligatory force in the specific case. CoE standards and national legal frameworks are mutually influenced.

In addition to the right to free elections, *other conventional rights* such as freedom of thought, expression and assembly and the prohibition of discrimination (articles 9 to 11, 14 ECHR and P12-1 to ECHR) are also relevant for elections but outside the scope of this

5 One exception is found in the European Union (EU) area: the European Parliament, which is the world's only directly elected transnational assembly. Note: the CoE includes all EU members.

6 See "Elections, referendums and political parties" or "Main documents" under https://www.venice.coe.int.

contribution. Additional instruments of interest developed by CoE include those on data protection, e-government.[7]

To be noted, the European electoral heritage contains *minimum principles* that apply throughout the region. Countries can do more and better. It goes without saying that all election-related procedures, whether low-tech and paper-based or high-tech and electronically backed, need to respect the minimum principles. Yet, the concrete application of high-level electoral principles to solutions based on ICT is not straightforward as digital solutions rely on logical abstractions, on algorithms, which can be understood only by a very small group of specialists.

Below we focus on the CoE standards for regulating e-voting and other uses of ICT throughout the electoral cycle, to the exception of uses related to opinion formation (e.g. ICT used for campaigning). Indeed, use (and misuse) of ICT for opinion formation purposes (e.g. microtargeting to influence opinions, use of opaque algorithms, etc.) are outside the scope of the instruments discussed below.[8]

3. Compliant regulation and use of ICT solutions in elections
3.1 The standard-setting process

Upon request by member States, the CoE gathered a group of national election practitioners and experts from academia to prepare the first Recommendation Rec(2004)11 on legal, operational and technical standards for e-voting. The Recommendation was adopted by the Committee of Ministers of the Council of Europe on 30 September 2004. Later (2010), it was supplemented by the Guidelines on transparency of e-enabled elections and the Guidelines for developing processes that confirm compliance with prescribed requirements and standards in the region (Certification of e-voting systems) which aimed at facilitating the practical implementation of the standards on transparency and certification. This first recommendation was the fruit of multidisciplinary work involving jurists, social science experts, IT specialists and practitioners from national EMBs. CoE offered thus countries access to a wide range of expertise. The group met regularly in biannual review meetings since 2004 and became the not-to-be missed forum for exchanging experiences between countries, academia,

7 The preamble of the 2017 Recommendation on standards for e-voting mentions a number of universal and regional instruments (hard and soft law) relevant to e-voting, including the Convention on Cybercrime (ETS No. 185); the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (ETS No. 108); the Additional Protocol to the Convention for the Protection of Individuals with Regard to Automated Processing of Personal Data regarding supervisory authorities and transborder data flows (ETS No.181) among others.

8 Opinion formation issues are dealt by other instruments of the Council of Europe. See e.g. European Commission for Democracy through Law (Venice Commission) and the Directorate of information society and action against crime of the Directorate general of human rights and rule of law (DGI), 2019, "Draft Joint Report on Digital Technologies and Elections", of 7 June 2019, CDL(2019)002.

etc. on issues related to e-voting and ICT in elections. In parallel, a scientific conference was created to steer academic research in this area.[9]

Based on experience through several e-voting pilots in the region and their evaluation, as well as on research by the academia, member States proposed an update of the Recommendation to integrate the lessons learned. A report on the need to update Rec(2004)11 and the associated Guidelines proposed a way forward.[10] The Committee of Ministers of the Council of Europe set up in April 2015 an "*Ad hoc committee of legal experts on legal, operational and technical standards for e–voting*" (CAHVE) with the mandate to prepare a new Recommendation updating Rec(2004)11 in the light of recent technical and legal developments related to e-enabled elections in the Council of Europe member States.[11] Member States and interested international organizations took active part in the discussions and consultations. Recommendation Rec(2017)5 on standards for e-voting, its Explanatory Memorandum, as well as the Guidelines on the implementation of the provisions of Recommendation Rec(2017)5 on standards for e-voting were approved by the Committee of Ministers in June 2017.[12] The 2004 Recommendation and the 2010 Guidelines on transparency and certification were repealed. Biannual meetings have been called and the CoE secretariat has continued the efforts to maintain exchanges between countries, in spite of challenges from internal restructurings at the CoE. While the Recommendation is meant to be a stable document, the accompanying guidelines are meant to evolve.[13] No work on the guidelines has been organised so far by CoE.

The process of elaborating guidelines on regulation of other ICT-backed solutions used in elections (other than e-voting and e-counting), started in 2019. Regulation of other uses of ICT in elections such as the e-backed registers and registering of voters, observers, etc., the collection of e-signatures, the e-poll books used in polling stations during voting day, the online transmission and publication of results, etc., was not really a topic of discussion until the U.S. 2016 Presidential election. That election marked a turning point. Documented foreign interference showed that ICT solutions like e-registers and e-registering could become targets and entry-points for attackers who seek to exert illegal influence over an election

9 The current E-Vote-ID conference is the successor of the initial EVOTE/Bregenz conference and the Vote-ID one. Both events merged in 2016. E-Vote-ID is held annually. More on https://e-vote-id.org/. At least one review meeting of the Recommendation was held during the Bregenz conference and academic experts and co-organisers of the conference were also core experts in the drafting of the CoE instruments on e-voting and ICT in elections.

10 The author of this article is the author of the report. An informal meeting of experts on the update was held in Vienna in December 2013 to discuss the report, https://www.coe.int/en/web/electoral-assistance/informal-meeting-of-experts-e-voting.

11 The author of this article was appointed lead expert for the elaboration of the new Recommendation on e-voting. She prepared a roadmap for the update and led the draft update of the Recommendation. Intermediary and final results were approved by CAHVE at its October 2015 and November 2016 meetings. More on http://www.coe.int/en/web/electoral-assistance/e-voting.

12 https://www.coe.int/en/web/electoral-assistance/-/council-of-europe-adopts-new-recommendation-on-standards-for-e-voting.

13 See also Driza Maurer (2017).

process. Fear of similar interferences sparked debate in Europe. The Netherlands banished use of counting and tabulation software shortly before the 2017 election and the security of results transmission software was much criticized in Germany. This cast a spotlight on their potential vulnerabilities and hence on their appropriate regulation. The CoE, under the aegis of its Committee on Democracy and Governance (CDDG), started working on a guiding instrument that would address regulation of all uses of ICT in elections, to the exception of e-voting, already dealt in Rec(2017)5. Use of ICT for opinion formation purposes (e.g. e-campaigning) was also excluded because it is qualitatively different: it involves players that are beyond the reach of electoral authorities (e.g. social media), whereas the ICT solutions covered by the 2022 Guidelines and the e-voting covered by 2017 Recommendation, are planned, introduced and supervised by the electoral authority.[14]

The CDDG was mandated to prepare a set of requirements and safeguards to be introduced in the legislation and practices of the Council of Europe member States when using ICT in the different stages of the electoral process with the aim of ensuring trust in elections. The CDDG made an important step by involving, beyond its circle of national experts, also the national election management bodies (EMBs) and other election experts, Venice Commission as well as academic core experts with legal, IT and social science backgrounds; a preparatory study "New technologies in the electoral cycle. Guidance from the CoE" was produced and presented to the CDDG working group on democracy and technology (GT-DT).[15] The CDDG Secretariat developed a questionnaire and distributed it to countries, including to national EMBs (end 2020). A summary of the answers to the questionnaire was discussed by GT-DT in February 2021. In particular, the type of technology to be addressed was debated. The academic experts presented a first proposal for the content of the Guidelines to the CDDG plenum in April 2021. National election experts and EMBs were consulted on the first draft. Their feedback was considered, and the guidelines were updated by the experts. A detailed informal discussion with EMBs and other national electoral experts as well as Venice Commission took place at the GT-DT meeting of May 2021 where each of the draft Guidelines was presented and discussed. Decisions on how to deal with feedback were based on broad consensus. The Guidelines were further iterated afterwards following a second consultation with member States (July-August 2021) and a final detailed discussion (September 2021). Eventually, they were approved by the Committee of Ministers (Ministers' Deputies) and became effective on 9 February 2022 (Driza Maurer et al., 2022).

14 Furthermore, ICT for opinion formation is discussed in other CoE documents. See Venice Commission (2004).

15 The author of this article was appointed lead expert for the elaboration of the Guidelines on ICT in elections. She is the author of the preparatory study. An abridged version is found in Council of Europe. (2020).

3.2 The standards

Below we introduce the main standards contained in the two instruments (Driza Maurer, 2017). The 2017 Recommendation on e-voting and the 2022 Guidelines on ICT in the electoral cycle are complementary and aligned. The Recommendation covers e-voting, which is the use of electronic means to cast and/or count the vote (including e-voting in polling stations, e-counting as well as internet voting) whereas the Guidelines on ICT cover all other ICT-backed solutions used in elections, to the exception of those related to opinion formation (see above). The Guidelines being much broader in scope, they are relevant also to e-voting. The opposite is not necessarily true: the standards of the Rec(2017)5 are specific to e-voting processes and may not fully apply to other ICT-backed processes.

In a nutshell, the Recommendation on e-voting provides guidance on the implementation of universal, equal, free and secret elections, as well as on gradual introduction of new technologies, accountability (certification, audits), distribution of responsibilities between state authorities, the private sector and the electorate, transparency and observation, reliability and security, data standards as well as handling of sensitive data, and interoperability (Annex I of Rec(2017)5). The Guidelines on ICT in elections deal with alignment of ICT with constitutional principles (G1), usability and accessibility (G2 and G3), integrity and authenticity (G4), availability and reliability (G5), secrecy and confidentiality (G6), transparency (G7), evaluation (G8), risk management (G9), member States necessary administrative and technical capacities (G10), member states responsibility (G11), dealing with exceptional circumstances (G12). Security is a cross-cutting issue dealt with in several guidelines.

Alignment with constitutional principles

The first recommendation (i) and the first guideline (G1) are about alignment of ICT with the principles of democratic elections and all other relevant constitutional principles that apply. Compliance with the principles is mandatory. To be noted, the list of principles mentioned in the Preambles of both instruments includes only minimum ones (European electoral heritage). Additional principles and requirements that apply at the national or local levels should, as well, be implemented and respected by the solution. In other words, compliance with the European standards alone is not sufficient; national and, as the case may be, local principles apply to the use of e-voting in a specific context and should be considered when deriving detailed requirements. This task, as well as that of ensuring that requirements comply with higher principles and are kept up-to-date, fall on member States (see standard 36, Rec(2017)5).

Regulation comes first

Drafting a compliant regulation and keeping it up to date is the starting point in achieving compliance of the ICT-backed solutions (and of any other solution). A Venice Commission report on electronic voting noted in 2004 that while e-voting is neither generally permitted

by human rights nor ruled out a priori, its acceptability depends primarily on its regulation, which must take particular account of the principles as well as of the technical and social conditions (Venice Commision, 2004).

One illustration of the importance of introducing regulation first (before the ICT solution) is the following. Some constitutional principles are contradictory. See for instance the opposition between secrecy on one hand and verifiability or transparency on the other. We want both. However, it is impossible, for any solution, to reflect both secrecy and verifiability to 100%. In such a case, the aim should be to ensure a fair balance which respects the essence of the principles. Defining such essence (minimum level) and deciding what is a fair balance between contradictory principles is a matter of legal evaluation and thus for the legislator to decide first. Given the specificities of ICT, it is often not recommended to transpose solutions that were agreed for paper-backed processes to the e-backed ones. A dedicated legal solution should be taken, and it should precede and indeed guide the development of the ICT solution.

Universal and equal suffrage

To ensure compliance with the principle of universal suffrage, the following objectives must be met according to Rec(2017)5: an e-voting system shall be easy to understand and use by all voters (standard 1); it shall be designed, as far as practicable, to enable voters with special needs and the disabled to vote independently (standard 2); in case of remote e-voting, this channel shall be only a complementary and optional one unless and until it is universally accessible (standard 3); and, in case of remote e-voting, voters' attention shall be drawn as to the validity of their e-vote (standard 4). The focus is on accessibility. Standards deal with the ergonomics of the interface, its interaction with the voter, access for voters with special needs (while at the same time maintaining an adequate level of security), universal accessibility (which, in our opinion, also includes voter understanding of how to conduct the security-related steps) and drawing the voter's attention to the official nature of the channel and the binding effect of the vote. Ensuring that these standards are met is not only responsibility of the competent authority: it also requires the active participation and contribution of the voter.

The Guidelines to Rec(2017)5 recommend that voters should be involved in the design of the e-voting system. The 2022 Guidelines require ICT solutions to follow a human-centered development approach and continuous improvement by collecting users' feedback. When e-solutions used in elections are not universally accessible, broadly accessible alternatives need to be provided too. For instance, according to Rec(2017)5, i-voting should only be an additional and optional voting channel as long as it cannot be accessed and used by every voter.

Equal suffrage mandates equality between several voting channels that co-exist. This is about equality of content or having the different channels present the voter with the same information and options. E-voting should not introduce any discrimination in this respect (omission or addition) although, technically speaking, it can offer more information than paper-based voting. Equal display is also important, to the extent that it may influence a

voter's opinion and should not be left to technical personnel alone to decide. Then, it is about making sure that the results from all voting channels flow into the final, consolidated result as well as about ensuring that the one-person-one-vote rule is respected, even when several voting channels are used.

Free and secret suffrage

Free suffrage means that the voter has the right to form an opinion and to express it in a free manner, without any coercion or undue influence. Distant voting methods are usually accepted under conditions. E-voting standards focus mainly on two aspects: on one hand, the configuration of the system so that it does not influence the voter's opinion and, on the other, the communication between the system and the voter and the different verification possibilities a voter should be offered to make sure the system or channel has not tampered with his or her vote. Procedural steps must make sure that all the information entered during e-voting and presented to the voter through the e-voting interface is authentic, namely identical to that provided by the competent authority. The e-voting procedure should be organised in such a way that makes voting inadvertently impossible. Messages addressed to the voter, thinking and reaction times, confirmation of choices, etc., should be configured to respect the voter's free expression of his or her opinion. Unlike other channels, an e-voting system should inform a voter who issues an invalid vote of the consequences and the possibility of casting a new vote if invalidity was not intentional. The Recommendation introduces verifiability mechanisms which develop the concept of chain of trust in e-enabled elections. They include verifiability tools which enable the voter to verify that his or her e-vote was cast as intended and recorded as cast, and that no vote was cast on her name (if she did not vote). These are known as *individual verifiability*. Rec(2017)5 introduces furthermore verifiability tools which allow any interested party to verify that votes are counted as recorded, and that all eligible voters' votes, and only them, were included in the result, also known as *universal verifiability*. The voter-verifiable paper audit trail produced by an e-voting machine used in a polling station or the return codes used in Internet voting are the two best-known examples of individual verifiability. Universal verifiability requires specialised knowledge and dedicated hardware and software and is usually conducted by trusted experts.

The other aspect of free and secret suffrage, which is for the voting system to prevent voter coercion and to ensure vote secrecy during vote casting, is impossible to ensure when remote voting systems are used (e.g. i-voting or postal voting). The Recommendation introduces a general requirement of secrecy of the vote, throughout the procedure and of encryption in the case of remote voting and pays special attention to data protection, however coercion and breach of secrecy during the casting of an i-vote (as well as of a postal vote) cannot be excluded. To mitigate this risk, Estonia has introduced the possibility of 'multiple voting', where the last vote overrides the previous one, allowing the voter to re-vote when the coercer is absent. However, this is a compensation, not a real protection of the voter's secrecy or freedom. Discussion is ongoing on the acceptability of coercion and breach of secrecy during vote

casting. One suggestion is to have, first, a proper evaluation of Estonia's long experience with multiple voting during internet voting.

Another *lex imperfecta*, is the requirement of the Recommendation that the voter should not receive proof of what he or she voted for, in order to prevent a breach of vote secrecy as well as vote selling. At the same time, the Recommendation requires that the voter receives information that allows them to check that their vote has not been tampered with and has been cast, transmitted and recorded as intended (individual verifiability). There is a contradiction between the two requirements which can be solved up to a certain point for voting machines (by prohibiting the photographing of votes and the taking the paper trail outside the polling station) but cannot be solved during internet voting, in the current state of technique. The Recommendation requires the State to inform the voter of the risks and protection possibilities. Information about risks is important but up to what point is it admissible to transfer the responsibility of securing the vote from the system to the voter (who should now make sure that he/she casts the vote in secrecy and without coercion)? This question is not answered in the Recommendation. It is an important legal question though, about the definition of secrecy. It should be decided by the national legislator.

The 2022 Guidelines underline that data-protection principles, like privacy by design and data minimization, are minimum requirements which need to be considered by the regulator. Those electoral data that qualify as "sensitive data" require the adoption of specific measures that go beyond data protection ones. Such specific measures should be included in the relevant electoral legislation. Additionally, long-term secrecy, i.e., post quantum secrecy and confidentiality, need to be considered as well.

Security and risk management

Rec(2017)5 requires member States to adopt appropriate measures for assessing and countering risks (rec. ii). According to the 2022 Guidelines, security is not just one principle among others, it the assurance that each of the principles will be upheld. Therefore, trust assumptions are already considered in G1. Some guidelines address security properties such as integrity and authenticity (G4),[16] availability (G5),[17] secrecy and confidentiality (G6). Furthermore, G8 requires a security evaluation and G9 requires to justify why the underlying trust assumptions are acceptable. The Preamble of the Guidelines stresses the importance of a human-centred security-by-design approach, of adjusting risk assessment to each phase of the election cycle, of conducting continuous risk management based on predefined criteria

16 Integrity checks should be provided throughout all relevant phases of the election to detect unauthorized changes. ICT solutions can also be used to identify irregularities (e.g. statistical checks such as risk-limiting audits), in combination with other types of observations, informed by country specific expertise. CoE Guidelines mention thus, for the first time, risk-limiting audits (G4).

17 If introduced and used, ICT solutions should be available and reliable, i.e., in line with the requirements and assumptions, even in case of system failures, user errors or attacks, and retain its functionality regardless of both hardware and software shortcomings. Alternatively, information on fallback solutions and channels should be put in place (G5).

for risk acceptance and a predefined methodology, of using ICT solutions that are state-of-the-art and based on peer-reviewed algorithms and concepts which are broadly endorsed by the respective scientific community.

Let us comment briefly on trust assumptions as this is quite a new concept in the electoral field. It is dealt with in guidelines G1 and G9 (see also the Glossary in the Guidelines). The security of each system relies, to a certain extent, on assumptions. It is indeed impossible or exorbitantly expensive to secure each and every aspect of a complex system like e-voting. Hence, certain aspects are considered to behave in a given way (e.g. assumptions about the ability of the voter to use verification tools, or assumptions about the [limited] capacities of an attacker, etc.). Only if the assumptions are upheld in practice, can the expected security be ensured. Assumptions are thus important part of security. They should be made transparent (by the provider) and their realistic nature (whether they can be upheld in practice or not) should be analysed as part of the risk assessment and re-evaluated periodically (G9). Trust assumptions are an important input for the risk assessment, i.e. on the likelihood that a requirement will be violated. The main decisions on the level of security and the acceptability of risks should be taken by the competent authority, usually the legislator, and not left to IT providers or experts.

Controls, transparency, accountability and responsibilities

Both instruments have the same approach on controls. As explained in the 2022 Guidelines, independent experts should evaluate the ICT solutions before starting using them. They should do so in particular regarding solutions' security, usability, and accessibility. In addition to taking the trust assumptions into account, the evaluation approach should define clearly and make public the target of the control, the assurance level, results, and the persons involved in controls. Regulation should also define how to deal with changes after the initial evaluation. It should foresee the procedures to be followed (G8). A permanent evaluation is part of the risk management policy (G9). The risk management approach needs to be re-considered on a regular basis and made publicly available.

Transparency is a cross-cutting issue when it comes to ICT solutions, including e-voting. All main decisions in relation to regulation and use of ICT in elections should be made transparent, including the assessment of minimum level of fulfilment of principles, the assessment of the realistic status of assumptions, of risks and any other relevant step. All aspects of the election need to be transparent. All stakeholders should be informed about the use of ICT in the election process, its operation, its properties, and its assessment (G8). There is a long list of transparency measures in both instruments including providing access to documentation, structured data about the election process and enabling public scrutiny.

As summarised by Guideline 11, member States and involved third parties are responsible for the proper implementation and conduct of the election process. Third parties involved need to fulfil the same standards and expectations as the member States. The ultimate responsibility for the conduct of the election lies with the member State. As for accountability in

the sense of identifying who caused a problem and holding them accountable, it goes beyond what verifiability provides today. It is tricky to ensure in e-voting and is an area of research.

4. Impact, limitations and future developments

The CoE has done pioneering work with respect to the regulation of e-backed solutions used in electoral processes. It is the only international organisation to have set standards in this field. The 2017 Recommendation on e-voting and the 2022 Guidelines on ICT in elections identify requirements and safeguards to be introduced in the regulatory framework of member States whenever use of such ICT-backed solutions is envisaged. Indeed, the instruments, in particular the Rec(2017)5 and its predecessor Rec(2004)11 have been regularly used by countries in the region both when studying the introduction of e-voting and when regulating it, and, in one case, the recommendation was almost copy-pasted in the national regulation of i-voting (Norway).[18]

The Recommendation has introduced standards which are based on academic research. It has achieved regional consensus on issues such as the importance of verifiability, disclosure of trust assumptions, greater transparency including publication of source code, the adoption of an interdisciplinary approach when regulating e-voting and ICT in elections, etc. These approaches are relatively new and were very little, if at all, discussed in the electoral field with respect to other "traditional" solutions. The CoE instruments have provided welcomed guidance here.

Experiences and feedback from members States show interest in pursuing reflections and work at the CoE level on other challenging issues such as cybersecurity, digital identity, verification of the vote, contingency procedures in case of interruption of communication, etc. which, members feel, should receive more attention at the national legislative level (Driza Maurer et al., 2022).

To be noted, the Council of Europe's recommendations and guidelines only discuss principles and standards that are minimum and common to all countries. CoE standards are not a complete regulation of e-voting or of ICT in elections. They indicate a method to be followed rather than a ready-to-use solution. The national regulator should consider, in addition to CoE standards, also national and local principles that apply. Furthermore, the balancing of principles that contradict each other, the evaluation of trust assumptions and of risks may yield different results in different contexts.

Several questions are still open and subject to ongoing research (we mentioned accountability). Another issue relates to the fact that ICT yields mathematical proofs, whose integrity, for instance, can only be evaluated by experts with specific knowledge, not by the layperson.

18 For a detailed account of how the 2004 Recommendation has been used by countries in the region, see Driza Maurer (2013). See also Stein & Wenda (2014).

This raises the question of experts and of their role as election watchdogs. Use of ICT (based on mathematics) does not eliminate the need to trust, it just displaces it towards IT experts. What happens if experts disagree? The judge will need to decide at some point, however, the judge is usually no IT expert. Whether reliance on experts respects the requirement of public control over the election is an open question. So far, it has been answered differently by a few jurisdictions in Europe. The most discussed decisions, that of the German constitutional Court (2009),[19] and of the Austrian Supreme Court (2011)[20] rejected reliance on experts and required highly specific rules for a system that can be fully verified by people without technical knowledge and without help from experts.[21] However, Estonia and Switzerland have so far relied on experts, although this is still a topic of debate.

Another question is that of voters' role in securing the system (already mentioned above). The probability that verifiability techniques detect problems depends on their effective use by voters. Are voters aware and capable of assuming such a role (which requires that they make use of the verifiability techniques, are able to interpret the results and react in case the results show potential problems)? The so-called usable security is an area of research.

To conclude, the Council of Europe has put the spotlight on compliance of regulation of e-voting and other ICT for elections with the higher-level constitutional principles, namely of free and democratic elections and has introduced instruments offering guidance to countries and helping them make informed decisions on compliant use of ICT in elections.

Bibliography

Council of Europe. (2020). *Digital Technologies in Elections. Questions, lessons learned, perspectives.* https://rm.coe.int/publicationdigital-technologies-regulations-en/16809e803f.

Driza Maurer, A. (2013). *Report on the possible update of the Council of Europe Recommendation Rec (2004)11 on legal, operational and technical standards for e-voting*. https://rm.coe.int/168059be23.

Driza Maurer, A. (2017). Updated European Standards for E-voting. The Council of Europe Recommendation Rec(2017)5 on Standards for E-voting. In: Krimmer, R. Volkamer, M., Braun Binder, N., Kersting, N., Pereira, O. y Schürmann, C. (Eds.), *Electronic Voting. E-Vote-ID 2017. Lecture Notes in Computer Science* (pp. 146-162). Springer.

Driza Maurer, A., & Barrat, J. (Eds.). (2015). E-*voting case-law. A comparative analysis*. Ashgate/Routledge.

Driza Maurer, A., Volkamer, M., & Krimmer, R. (2022). *Council of Europe Guidelines on the Use of ICT in*

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

20 VfSlg. 19.592/2011, judgment of 13 December 2011

21 See Ardita Driza Maurer; Jordi Barrat (eds), E-*voting case-law. A comparative analysis*, Ashgate/Routledge 2015. See in particular the chapters on Germany and Austria.

Electoral Processes, in Computer Security. ESORICS 2022, International Workshops, Copenhagen, Denmark, September 26-30, 2022, Revised Selected Papers. S. Katsikas

Stein, R., & Wenda, G. (Eds.). (2014). Ten Years of Rec(2004)11 – The Council of Europe and E-voting. In: Krimmer, R., & Volkamer, M. (Eds.), *EVOTE 2014. Proceedings* (pp. 105-110). TUT Press.

Venice Commision. (2004). *Principles for a fundamental rights-compliant use of digital technologies in electoral processes*. Council of Europe. https://www.venice.coe.int/webforms/documents/?pdf=CDLA-D(2020)037-e.

Venice Commision. (2004). *Report on the compatibility of remote voting and electronic voting with the standards of the Council of Europe*. Council of Europe. http://www.venice.coe.int/webforms/documents/CDL-AD(2004)012.aspx.