COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Digital solutions in the electoral process

In the light of international standards and good practice

Ardita DRIZA MAURER

Legal expert, Council of Europe

30 April 2021

Study is developed within the Council of Europe Project: "Supporting Transparency, Inclusiveness and Integrity of Electoral Practice and Process in Georgia"

Disclaimer: The opinions expressed herein belong to the author and do not necessarily reflect the official position of the Council of Europe.

Contents

1 Overview

1.1 Assignment

The assignment was to study the introduction of certain digital solutions used in electoral processes from a legal and practical perspective, based on international standards, namely the Council of Europe standards, as well as on different countries' practical experiences. The pros and cons around the introduction of information technology in elections, recommended timelines and approaches for their introduction were also to be addressed. The study should also focus on digital solutions currently discussed and envisaged in Georgia in the areas of voter registration, voting and counting. It should furthermore offer recommendations, which may serve as a roadmap for national stakeholders in light of ongoing electoral reform in Georgia.

1.2 Methodology

Organic Law of Georgia, the Election Code of Georgia[1] (hereinafter - the Election Code), the draft law modifying the Election Code[2], and the Council of Europe Recommendation CM/Rec(2017)5 on standards for e-voting with its Explanatory Memorandum and associated Guidelines are the legal background of reference when considering the proposed development of digital solutions in elections in Georgia. Other documents are relevant, including the OSCE/ODHIR Handbook for the observation of new voting technologies, reports and evaluations from OSCE/ODIHR and Venice Commission, studies and suggestions on use of digital solutions in elections from IDEA, IFES and other international organisations.

The terms "ICT" (information and communication technology), "digital" and "high-tech" solutions will be used as synonyms throughout this report. ICT in elections points, first, to digitized documents and procedures involved in the electoral process. Digitization is the founding layer. Furthermore, it may also refer to the use of biometry, of blockchain, of cloud computing or of artificial intelligence.

[1] https://matsne.gov.ge/en/document/view/1557168?publication=65

[2] https://info.parliament.ge/#law-drafting/21736

The term “e-voting” has a general and a narrower meaning. The Council of Europe Recommendation Rec (2017)5 on standards for e-voting, defines e-voting as *the use of electronic means to cast and/or count the vote*. At this level, e-voting has a very general and broad definition and encompasses different types of solutions such as e-voting on electronic voting machines (EVMs) in polling stations, internet voting from home, as well as e-counting of paper ballots by counting machines such as optical scanners. However, in the present study, we will be more specific when discussing the different e-voting solutions: we will use the term *e-voting* to refer (mainly) to the use of EVMs. *I-voting* refers to internet voting and *e-counting* is used when discussing the e-counting of paper ballots.

This study focuses on the use of some digital solutions only, namely those discussed in the draft law: *voter authentication and registration*, *voting in polling stations* as well as *counting and results management*. The main questions to be considered when envisaging these solutions are discussed in chapters 4 and 5. Questions are examined in the light of relevant CoE recommendations and guidelines as well as countries’ good practice.

1.3 Structure of the study

Chapter 2 starts by presenting the legal situation in relation to the introduction of new digital technology in elections in Georgia. Then, it offers an overview of digital solutions used in elections in the CoE region, with a focus on *election management systems* which are the backbone also of voter authentication and registration, as well as on solutions for *voter authentication and registration* and on solutions for *voting* and for *counting ballots and managing results*.

Chapter 3 presents the legal instruments that are relevant and should be observed when addressing the use of digital technologies in elections.

Chapter 4 focuses on main steps required for the initial introduction of e-voting and e-counting solutions. A general strategy needs to be elaborated which must clarify the main directions. Stakeholders need to be consulted and closely involved in the initial reflection and in the development of the system. Introduction should take place gradually and must be preceded by detailed regulation of the testing phase. The detailed regulation should clarify the requirements that apply to the solution and the conditions for conducting the tests, as well as criteria for their evaluation. During the testing period the solution is used in a small scale and preferably starting with lower level elections. Evaluation of testing should be conducted on clear, scientific criteria. Its results will offer the competent authority the factual basis to decide whether to roll out the solution, or to adjust it and continue with additional tests, or to take note of its failure and stop the testing.

If the decision is to further develop the solution, the regulation of the test phase should be reworked to reflect lessons learned from testing as well as possible additional requirements related to the extended use/complete rollout of the solution. The regulation for e-voting and e-counting should be detailed enough to accurately translate the higher-level principles for democratic elections into requirements for these solutions. Chapter 5 delves into some main aspects to be addressed by the detailed regulation including description of functionalities, requirements for accessibility, usability, secrecy or rather confidentiality, verifiability, controls and evaluation, transparency as well as public authorities' oversight and the role of private sector providers. A risk management policy framework should be adopted when ICT, in particular web-facing solutions, are used. Furthermore, the regulation should clarify how disputes and remedies are handled when digital solutions are used. The procedure for handling incidents and communicating about them, need to be foreseen. The continued evaluation of solutions needs to be discussed, given the fact that technology-related risks and opportunities evolve in time. And so, do people's perception of technology as well as electoral law in general.

The sustainable use of ICT in elections is a crucial issue. It should be addressed from the beginning of the process when a strategy and initial regulation are envisaged. The question of upskilling voters, staff, observers, etc. so that they gain a good understanding of the ICT solution and are enabled to exercise their rights and duties is yet another important aspect. Finally, the issue of public trust in the ICT solutions and ultimately in the election needs to be discussed.

By way of a conclusion, Chapter 6 offers some recommendations to Georgian authorities, based on international standards and good practice, on introducing ICT solutions in compliance with the principles for democratic elections.

2 Digital solutions used in elections

2.1 Situation in Georgia

Improving election processes through introduction of technology systems is a common theme in many countries. Adaptation of the legal framework to govern such systems is increasingly discussed and its importance better understood.

The Government of Georgia has presented a draft law modifying several articles of the Election Code[3]. One of them, article 32 of the draft law says:

> *32. Paragraph 203^2 shall be added to the Law and formulated as follows:*
>
> *Article 203^2. Conducting certain actions through electronic means by the CEC during the transition period*
>
> *"1. For the next municipal elections, the CEC is authorized to carry out the procedures of registration of voters showing up at the polling station, voting, counting of votes and drawing up a summary protocol of the results through electronic means.*
>
> *2. The CEC shall ensure the registration of voters at all polling stations with an electronic registrar.*
>
> *3. The CEC shall ensure (a list of selected districts shall be added here) counting of ballot papers by electronic counter in at least as many precincts as is necessary to reveal the sociologically valid results of that constituency.*
>
> *4. The rules and conditions for the use of electronic means provided for in paragraph 1 of this Article shall be determined by the CEC resolution.".*

It follows from the reading of this draft provision that:

[3] https://info.parliament.ge/#law-drafting/21736

1. The CEC is *authorized* to introduce the electronic registration of voters (registration of the fact that they voted), e-voting, e-counting and the electronic drawing of a summary protocol of the results for the next municipal elections (para. 1).
2. When making use of this authorization, the CEC has the *obligation* to introduce e-*registration* of voters with an electronic registrar at *all polling stations*, whereas *e-counting* of paper ballots should be introduced *"in at least as many precincts as is necessary to reveal the sociologically valid results of that constituency"* (para. 2).
3. The introduction of *e-voting* is mentioned in paragraph 1, but is not developed further. It is unclear what kind of e-voting paragraph 1 refers to.
4. The CEC is mandated to *regulate all conditions* governing the new electronic processes through a resolution.

Accordingly, some of the questions that arise about the proposed regulation include:

1. What is the exact envisaged form of the different solutions mentioned in the draft law?
2. What is the exact purpose of introducing these specific solutions, namely what are the needs that are being addressed and what is the final goal? What are the expected results?
3. Are the foreseen solutions the best fit to achieve the stated objectives? Is the foreseen organisation adequate?
4. What are the detailed requirements that the solutions should fulfil?
5. What is the detailed organisation of the envisaged testing phase?
6. The cumulative roles of the CEC as regulator, implementer and evaluator of the digital solutions need in-depth consideration. The controlling of the technical solutions and of their implementation needs to be envisaged and regulated.

In assessing these and other questions, the relevant regulatory instruments should be clearly spelled out (see chapter 3).

No electronic solutions for voter authentication or registration, voting or counting are currently present in Georgia. The Election Code mentions a certain number of databases such as unified voters' list (article 31, Election Code), register of observers (article 40, Election Code), registration of press and media (article 44), register of parties (articles 113, 142, 197, 202, Election Code), as well as some electronic applications from electoral subjects, observers, media (article 14, Election Code).

2.2 Situation in the Council of Europe region

Today, almost every aspect of the election has some interaction with an ICT-backed system or process.[4] Electors' registers are ICT-backed and in some places the registering of electors takes place via the web. ICT-backed registers and registering of parties and candidates, online training of observers, of election administration staff, and of electors; e-identification of voters and registration of their participation (e-pollbook), e-voting (on EVMs in polling stations or over the internet), e-counting (programmes that register and calculate results), e-transmission of results from local to central authorities, results management systems (including seat allocation), solutions for performing checks and statistical analysis, systems for managing claims and disputes, etc. are some examples of the use of ICT-backed solutions in elections in the region. The list is by no means exhaustive.

At the technology level, the digitization of documents and processes is the first, founding layer. ICT however also refers to the use of biometry, blockchain, cloud computing, or artificial intelligence. While e-voting and e-counting have received a high level of attention since the beginning of the years 2000,[5] use of ICT for other purposes during the electoral processes has been less studied. The Council of Europe is pursuing its pioneering work in the area of regulation of use of ICT in elections and currently working on establishing guidelines for the use of ICT throughout the electoral process.[6]

In some CoE countries, use of ICT may be expressly excluded for some processes. For instance, with respect to voting or counting, the use of ICT to yield official results is forbidden in Austria.

[4] OSCE/ODIHR, *Handbook for the observation of new voting technologies*, 2013

[5] The Council of Europe has done pioneering work by introducing guiding instruments that clarify the application of electoral principles when e-voting is used. A first Recommendation on legal, operational and technical standards for e-voting was adopted in 2004 and later completed with guidelines on certification and on transparency of e-voting solutions. These instruments were eventually replaced by the new Recommendation on standards for e-voting, CM/Rec(2017)5 (see chapter 3).

[6] The author of this study advises the CoE Committee on Democracy and Governance (CDDG) in developing standards on new technologies and the different stages of the electoral process (including voter registration, transmission and tabulation of results, etc.) in the form of a Committee of Minsters' recommendation or guidelines https://www.coe.int/en/web/good-governance/democracy-and-technology

In this case, ICT-backed solutions are only used to assist the authorities in establishing preliminary results but not for establishing final results whose processing remains manual. Elsewhere, some uses of ICT-backed solutions are strongly recommended or even required for certain groups of the electorate such as the sight-impaired, the expatriates, etc. In Croatia for instance, use of some ICT solutions is required for certain minorities.

2.2.1 ICT solutions during the electoral processes

Below is a snapshot of use of ICT solutions during the main phases of an election. In the next sections we discuss some of these examples.

Election Phase	**Main users**	**System, solution**
Pre - Elections	Electors	Online registration in the electoral system Verify registration Consult assigned polling station Change polling station Apply for a special voting method (e.g. when in a hospital) Sign a referendum/initiative demand Sign in support of a candidate/party
	Election administration	Boundary delimitations Voter card printing Electronic ballot generation system
	Parties Candidates	Online political party registration system Electronic Candidate Nomination System
	Parties'agents Media Observers Translators	Online application system Online accreditation system
	Electors, Election administration staff	Online Training Systems
Election Day	Staff	Electronic journal
	Voter	Voter authentication
	Staff	Voter registration (local e-pollbook)

	Staff	Voter registration (central e-pollbook) and electronic data exchange btw polling stations and central database
	Voter	E-voting at polling station (EVM) or from a distant place (internet voting)
	Staff	E-counting of paper ballots
	Staff	Electronic Results transmission
	Staff	Centralised Results Management System
Post Elections	Voters, candidates, election authorities, judicial system, etc.	Dispute resolution management system
	Staff / observers / other	Statistical audits

Below we focus only on some of them.

2.2.2 Election management system

Almost all countries in the CoE region have some digitized key election data. Georgia, as mentioned, has several e-registers. Initially, most EMBs started introducing varied systems and solutions for handling documents and processes, such as registers. As technology and the understanding of the technology by EMBs evolve, these are increasingly making use of integrated services and systems, called Election Management System (EMS). EMS include several services/systems some of which may be used by decentralised entities (e.g. regional and local election administration staff) but communicate with centralised databases which consolidate information. Databases, web applications and other programmes are part of such systems.

One of the main components of an EMS are registers, e.g. register of electors, of political parties, of candidates, of observers, of party representatives, of interpreters authorized to assist international observers, of trained and certified persons, of appointed electoral staff, of appointed IT assistants, who operate / assist staff that operates ICT solutions introduced in polling stations, of third-party campaigners (stakeholders, other than parties, that promote or oppose a referendum and actively campaign for/against it), etc. Stakeholders have the right to consult and modify the information included in the mentioned registers, to apply to register, etc. Where several registers exist (e.g. at the different levels of the state), a periodical audit of decentralised registers (data match functionality) is organised to maintain completeness and accuracy of electoral registers. Alternatively, continuous data matching against local data sources is done to maintain accuracy.

The CECs extensively use such systems to communicate with stakeholders outside the election administration, such as voters, parties, candidates, observers, media, etc. Additionally, the CEC increasingly relies on ICT solutions during all phases of the election administration. E.g., during the preparatory phase, ICT is used to register and update polling stations and other electoral units, administer lower level election administrations, distribute ballot papers and other material; generate and transmit decisions relating to lower level commissions such as appointments of staff; keep updated information on trained and certified persons, appointments of staff, IT assistants, etc. to a specific polling station, etc.; verify signatures in support of a candidate; perform candidate validity check; check the application of established gender quotas by political parties; generate ballots, collect signatures and verify data from signature collection (on issues); disseminate all kind of information through its web pages and social media accounts; live stream activities for the purpose of transparency, etc.

Several countries have plans to further extend use of EMSs by including new components, developing and streamlining existing ones, etc. *Denmark* and *Finland* are working on a new election management (or information) system, *France* envisages the development of a system to collect e-signatures for referendums, *Ireland* has an electoral register modernisation project.

2.2.3 Voter e-authentication and e-registration on voting day

Voter authentication and voter registration systems are some other digital solutions used on voting day in polling stations. Voter authentication on “smart devices” in polling stations is used in a few cases in the CoE region, e.g. in Armenia since 2017. It was experimented recently in Albania (April 25, 2021 parliamentary elections). The smart device includes a database with voter information, including biometric information, against which the identity of the voter is checked. The system also registers the fact that the voter votes. A general database of electors (electors’ register) is necessary for preparing the data to be loaded on the voter authentication smart device, as well as for the consolidation of data collected at polling stations, their examination and elaboration of reports.

E-registration of voters, i.e. registration in an e-pollbook of the fact that they voted, is done in many cases throughout the region, independently from e-authentication, and based on the “traditional” authentication of the voter. In a few cases, the information registered at the polling station is transmitted ongoing to a central database which communicates with all polling stations. This allows to control and prevent multiple voting in the case where the voter is not bound to one polling station but has the option to vote anywhere in the country. Such a solution requires good network connections between polling stations and central databases, among other conditions. *Latvia* and *Poland* for instance have piloted, respectively envisage an ICT-backed solution providing the possibility for voters to vote at any polling station.

2.2.4 E-voting in polling stations

There are mainly two distinct types of ICT solutions for voting purposes: e-voting machines (EVMs) in polling stations and i-voting from an uncontrolled environment, via the internet. Here we discuss the first group of solutions.

E-voting or the e-casting of the vote on a voting machine is practiced in a few countries in the region, including in *Belgium*, for all kinds of elections and referenda, in some 66 *French* communes, or in *Russia*, for national and regional elections. The use of e-voting machines has been partially or totally suspended or abolished in *Bulgaria* in 2019, for local elections, due to the complexity of such elections and the related financial cost for developing an ad-hoc e-voting solution. It was suspended in *Finland* after the 2008 municipal election trial where voters were confronted with usability issues which prevented them from completing the voting process; it was suspended partially in *France* where, since 2008, a moratorium prevents any extension of e-voting to new communes; in *Germany* where the Federal Constitutional Court decided in March 2009[7] that the use of e-voting machines, as practiced in Germany at that time, was incompatible with the principle of the public nature of elections according to which the layperson must be able to follow and understand the main steps in the election process without special technical knowledge; in *Ireland* in 2008; in *the Netherlands*, where, following decades of use of EVMs, they came under heavy criticism in 2006 for lack of secrecy and auditability and where, since 2008, all voting is held using only paper ballots.

When using e-voting machines in polling stations, the use of paper ballots as a second medium to store the vote for verification purposes is strongly recommended. The voter-verified paper

[7] BVerfGE 123, 39, https://www.servat.unibe.ch/dfr/bv123039.html

audit trail (VVPAT) feature of the EVM prints the voter's selections on paper and allows the voter to confirm his/her selections by inspecting this paper before the vote is cast. The paper record is preserved and, depending on regulation, may serve in the event of an audit or recount which is a manual re-count of paper votes. These are carried out to gain assurance that e-voting machines or counting ones are not corrupted. A generation of EVMs which offers VVPAT is used in *Belgium*.

A more complex form of verifiability is end-to-end verifiability (E2EV) which involves the use of cryptographic solutions to ensure both vote secrecy and verification of voting rights. E2EV encompasses the following three steps: (1) *cast-as-intended*, i.e. a voter can verify that a ballot is cast correctly for the intended candidate; (2) *recorded-as-cast*: a voter can verify that a cast ballot is recorded correctly in the system; (3) *tallied-as-recorded*: a public observer can verify that all the recorded ballots are tallied correctly and only eligible voters' votes were included in the final result and none of them was destroyed. The first two steps are also known as individual verifiability. The third one is also known as universal verifiability. E2EV is used primarily in internet voting. Systems like those used in *Norway* and in *Switzerland*, as well as the one in use in *Estonia*, offered, respectively offer some form of E2EV. Recently, the *United Kingdom* experimented a new, end-to-end verifiable voting solution for e-voting in a polling station.[8] The experiment took place in a non-binding trial held during the local elections of May 2019 and may provide indications on how electronic voting in polling stations could look like with end-to-end verification possibilities.[9]

Legacy, first generation black-box e-voting systems in polling stations are being questioned. Legal and technical developments have contributed to setting the bar for security and transparency much higher, with end-to-end-verifiable voting solutions and general transparency (source code publication, etc.) becoming standard requirements for e- or i-voting in the CoE region.

[8] https://www.bbc.com/news/technology-48132591

[9] Fang Hao *et al*., "End-to-end Verifiable E-voting Trial for Polling Station Voting", available at https://eprint.iacr.org/2020/650.pdf

2.2.5 E-counting and e-results management

Counting, results transmission and results management, controls, seats allocation, etc. are typical areas where ICT solutions are extensively used, in probably all countries of the CoE region. Here are a few examples.

E-counting of paper ballots via optical character recognition technology is practiced in *Hungary* (for preliminary results only), *Latvia, Malta, Norway,* in some *Swiss* cantons for referenda, in the *Russian Federation* and in the *United Kingdom.* In this last case, e-counting was used in *England* in 2000, 2004 and afterwards, in local and national elections. *Scotland* used it at the 2007 national elections and at the 2012 and 2017 local elections drastically reducing the counting time of the ballot papers from three or four days to a matter of hours (Single Transferable Vote system).

E-transmission and centralized e-management of results are used to speed up election results consolidation and publishing. The process of results data transmissions from polling stations to central databases provides the EMB with the ability to publish preliminary results relatively quickly after the closing of polling stations. As with centralised pollbooks, the reliance on high available networking is of critical importance for e-results transmission.

Solutions for the transmission of provisional and/or final voting results from the manual counting at polling stations to central entities are used in *Austria, Azerbaijan, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Greece, Germany, Hungary, Latvia, Norway, Romania, Slovak Republic, Slovenia, Spain, the Netherlands*. In *Ireland, Scotland* and *Malta* software assisting the returning officers with ballot box recording and accounts in accordance with the system of Proportional Representation-Single Transferable Vote (PR-STV) is used. Seat allocation software is used in the *Netherlands, Norway* etc. Solutions for handling results include checks for identifying arithmetical errors regarding the data written down on the paper-based election protocols. Any mismatch between figures is flagged by the application. As a precautionary measure, the software may be designed not to allow for immediate data transmission in cases where figures do not reconcile (*Romania*). Statistical audit methods for checking the plausibility of results are used in post-election audits. E.g. risk-limiting audits are increasingly being used/recommended in the *USA*.[10] Final scrutiny of results is assisted by a computer application in *Spain*: three days after the election, a final scrutiny of the votes in paper sent by each polling station is carried out, in which the Electoral Boards are assisted by this application. Registration and ongoing publication of data on voter turnout (preliminary and final results) is commonly found in all cases.

2.3 Increased use of digital solutions in the current pandemic?

The outbreak of COVID-19 has confronted elections management bodies with uncertainty and unknowns about the organisation of elections. For instance, at the start of the pandemic, many countries postponed elections, however from June 2020, the trend shifted to holding elections. As 2020 progressed, election management bodies had more time to prepare and implement response mechanisms, and to conduct voter outreach programs aimed at reassuring voters anxious about participating, more and more elections went ahead on schedule. Examples include Croatia, Italy, Kyrgyzstan, Lithuania, the United States.[11] Elections were held in Georgia on October 31st and, apparently, election activities did not have a direct clear impact on COVID-19 cases.

Several countries in Europe have sought to adapt and expand existing models of voting to accommodate the needs of voters in quarantine or in isolation as well as to reduce the risk to get infected for voters, observers and staff. Increased use of ICT has often been mentioned as a means of facilitating different aspects of the organisation of elections during the current pandemic. But has there been an enhanced use of ICT? Below are examples from the CoE region.

Campaigning has transferred mostly online. Other processes as well. Electors in some countries were able to apply online for a specific vote modality (e.g. for postal voting where this

[10] https://www.cartercenter.org/resources/pdfs/peace/democracy/ask-an-expert-postelection-audits.pdf

[11] International IDEA documents the impact of the COVID-19 pandemic on the conduct of elections. See https://www.idea.int/news-media/multimedia-reports/global-overview-covid-19-impact-elections . Exchange of practices between European EMBs on special voting arrangements (SVAs), see https://www.idea.int/news-media/news/exchange-practices-between-european-embs-special-voting-arrangements-svas

possibility was given, or for changing voting location). In this case, the voter had to authenticate him/herself electronically, by using an e-signature, or other codes (e.g. *Spain, Latvia*, *Croatia*). Training activities for electoral staff, observers, voters, etc. have been transferred online as well. Web-based training seems to have become a lasting solution in several countries (e.g. *Croatia, Latvia, Moldova, Romania*). Strengthening online information of the public and adapting existing ICT solutions to accommodate new, pandemics related needs is another general development trend.

In most countries, short term introduction of new ICT-backed solutions as a quick answer to COVID-19 related challenges has not been chosen as applicable, mainly due to the short time available in the context of the current pandemic. Countries are now envisaging respectively introducing longer-term strategies and regulations to deal with possible future pandemics and other emergencies. Emphasis has been put on increasing the flexibility of the existing, mostly manual, procedures. The discussion about e-voting methods has been renewed in several countries (e.g. *Lithuania* or *Moldova*). The potential of the internet to contribute to the exercise of direct democracy rights (launching initiatives and referendums) during a pandemic is debated in *Switzerland*, *Croatia*, etc.

The CEC of Georgia introduced several measures to address COVID-19 related challenges during the last elections.[12] The evaluation was overall positive and there was consensus that elections were managed efficiently, despite challenges posed by the COVID-19 pandemic.[13]

3 Relevant regulatory instruments

3.1 International standards and good practice

Elections, and technologies used in elections, should respect several principles and conditions that lend them the democratic status, namely the principles of free and democratic elections. These include the right to universal, equal, free, direct and secret suffrage, periodic elections and their publicity as well as the conditions for implementing these principles, such as

[12] See the following four decrees: https://cesko.ge/res/docs/decree45.pdf ; https://cesko.ge/res/docs/decree43.pdf ; https://cesko.ge/res/docs/dadg38ing.pdf ; https://cesko.ge/res/docs/20200922225145decree24.pdf

[13] OSCE/ODIHR final report of 5 March 2021 https://www.osce.org/files/f/documents/1/4/480500.pdf

procedural guarantees of impartiality, transparency and observation.[14]. Freedom of expression, non-discrimination, freedom of movement, freedom of association etc. should also be complied with. However, ensuring compliance with free elections is the most challenging part and the focus of this study.

The principle of free elections is foreseen in binding international instruments, namely article 21 of the 1948 United Nations Universal Declaration of Human Rights (UDHR),[15] article 25 of the 1966 UN International Covenant on Civil and Political Rights (hereinafter – ICCPR) and article 3 of the additional (first) Protocol to ECHR (hereinafter P1-3 ECHR). Authoritative interpretations (e.g. ICCPR's General Comment 25), the case law of ECtHR namely on P1-3, political commitments such as the 1990 Copenhagen Document of the Conference for Security and Co-operation in Europe (CSCE) interpret and complete the list of elements of free elections. The Charter of Fundamental Rights of the European Union contains similar rights and applies to EU countries. Pursuant to P1-3 ECHR[16] and case law of the ECtHR, the State has the positive obligation to make sure that all activities led by it within an electoral cycle, including those backed by new technologies, comply with the mentioned principles.

Details about the exact meaning of electoral principles are to be found in the 2002 Code of Good Practice on Electoral Matters and the 2007 Code of Good Practice on Referendums of the European Commission for Democracy through Law (Venice Commission) of the Council of Europe. These two documents, although soft law, play an important role and are considered as a benchmark by national legislators and courts. The European Court of Human Rights refers to them when interpreting P1-3 for instance.

The use of *digital technologies* in elections, calls, additionally, for other tech-related legal instruments like the Convention on Cybercrime of the Council of Europe (Budapest

[14] See Venice Commission, Code of good practice in electoral matters, Opinion No. 190/2002, adopted by the Venice Commission at its 52nd session (Venice, 18-19 October 2002); CDL-AD (2002) 23 rev.

[15] The UDHR is not a treaty; however, its provisions are universally accepted and considered to be customary international law.

[16] 45 out of 47 member states have ratified this protocol. Switzerland and Monaco have signed it but not yet ratified. However, to the exception of the accepted lack of secrecy in (only) some local elections where voting by raising hands is used, electoral principles of Swiss law are usually considered to be stricter compared to P1-3 ECHR.

Convention), the Council of Europe Modernised Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108+) and the EU corresponding instrument, Regulation (EU) 2016/679, General Data Protection Regulation (GDPR).[17] EU legislation on cybersecurity is emerging, as shown by the 2016 Directive on the security of network and information systems (NIS Directive) which is the first piece of EU-wide legislation on cybersecurity. It was followed by the EU Cybersecurity Act adopted in 2019 which introduces, for the first time, an EU-wide cybersecurity certification framework for ICT products, services and processes. These instruments are relevant in the region.

Opinions, observation reports, and other documents on the use of ICT in elections, by Venice Commission, OSCE/ODIHR, Council of Europe's Parliamentary Assembly (PACE), etc. are relevant too. The EMBs Conference[18] organised by Venice Commission has repeatedly dealt with issues related to use of ICT in elections. Ongoing work by the European Committee on Democracy and Governance (CDDG) in the field of use of ICT in elections is also relevant.[19]

All the above-mentioned international instruments and interpretations present general principles for democratic elections which apply regardless of the technology used. According to article 3 of the additional Protocol to the ECHR, the legislator has the task to actively introduce regulations that ensure that only digital solutions which comply with the higher-level principles can be used in elections.

The question is how to write such regulations? How to translate the principles in detailed requirements and make sure that technology complies with such requirements and, ultimately, with the principles? This is not an easy task because it requires combined legal and technical expertise. The field is still experimental. Guiding instruments that clarify the application of

[17] Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation), which became directly applicable across the European Union on 25 May 2018. According to the European Commission, it provides the European Union with the tools necessary to address instances of unlawful use of personal data in the electoral context.

[18] https://www.coe.int/en/web/electoral-management-bodies-conference

[19] https://www.coe.int/en/web/good-governance/democracy-and-technology See also relevant work at https://www.coe.int/en/web/electoral-assistance/e-voting

electoral principles to the use of ICT in elections have been introduced by the Council of Europe which has done pioneering work in this area, since 2004.

Recommendation CM/Rec(2017)5 on standards for e-voting,[20] its Explanatory Memorandum[21] and the associated Guidelines[22] are the main legal backdrop, both for e-voting and for other uses of ICT in electoral processes. They are meant to guide authorities when drafting the legal basis that should regulate e-voting, e-counting or other ICT. Another practical resource is the OSCE/ODIHR Handbook for the observation of new voting technologies.[23]

The CoE Recommendation CM/Rec(2017)5 enlists 49 standards which set objectives that e-voting should fulfil to comply with the principles and conditions for democratic elections, the so-called European electoral heritage. Detailed guidance is to be found in the Guidelines on the implementation of the provisions of CM/Rec(2017)5.

The Recommendation spells out what kind of requirements should be envisaged. However, the Recommendation only includes minimum standards applicable throughout the CoE region. Compliance with them can be seen as a first step. Member states should, in addition, refer to principles which are specific to their country and to the vote or election in which ICT will be used.

[20] Recommendation CM/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 2017at the 1289th meeting of the Ministers' Deputies). Available from https://rm.coe.int/0900001680726f6f

[21] Explanatory Memorandum to Recommendation CM/CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting, 14 June 2017 (CM(2017)50-add1final). https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168071bc84

[22] Guidelines on the implementation of the provisions of Recommendation CM/CM/Rec(2017)5 on standards for e-voting, 14 June 2017 (CM(2017)50-add2final), https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680726c0b

[23] https://www.osce.org/odihr/elections/new_voting_technologies

3.2 National legislation

Digital solutions being used in a specific national or local context, compliance with international standards is not enough. National and local legislation should be considered and specific legal principles, included. Georgia’s Constitution and laws, namely the Election Code and lower level instruments (decrees of CEC) apply to the whole electoral cycle, including to new digital solutions.

ICT solutions in elections should also be considered in the light of data protection and (cyber)security legislation. Furthermore, legislation addressing emergencies or pandemics may be relevant. Consultation and coordination with relevant bodies such as a national cybersecurity body or the data protection watchdog are necessary.

4 Organisation and timeline

4.1 General strategy

Before addressing the introduction of a specific ICT solution in elections, it is highly recommended that the Government, the Parliament and the Central Electoral Commission carry out a detailed analysis and decide the main aspects of the development of ICT in elections. Feasibility studies are usually conducted to evaluate the different aspects that are relevant.

The strategy will clarify ways and means in which ICT should be introduced and developed. It will take account of the electoral system as well as of broader aspects such as the development of e-government, of cybersecurity policies, etc. When deciding the strategy, costs, risks, perception of ICT solutions in elections among voters, systems’ continued maintenance and upgrades, technical support, etc. must be considered.

Strategic decisions should be furthermore informed by the needs and must set objectives for ICT solutions to address the needs. ICT may solve existing problems and bring enhancements (on efficiency, transparency, participation, etc.). Different groups of the electorate, e.g. the visually impaired, the expatriates, women, youth, etc. have specific needs. And so do other election stakeholders, e.g. parties, candidates, observers, election administration staff, etc. who interact with the solution or observe it have. Requirements on ICT solutions to address such needs and expectations need to be thought out.

4.2 Regulation of the testing phase

The legality principle requires that any ICT solution (similar to any other solution used in elections to produce official results), should be sufficiently regulated. The level at which this regulation is introduced (e.g. whether in the Constitution, in the law or in lower acts) as well as the level of detail of the regulation itself need to be considered.

ICT solutions should comply with the higher-level constitutional principles and the law. An adequate regulation is the first step towards a constitutionally compliant digital solution. Furthermore, the main aspects of the use of digital technologies in elections should be regulated in a solution-neutral way. Unfortunately, often regulation is considered after the solution has been selected or developed. This is wrong. Detailed regulation should drive the development of ICT solutions and not the other way around. This is so for all ICT solutions that produce official results, even if they are only used on a small scale and in a limited manner (test phase).

The CM/Rec(2017)5 spells out elements that should be taken into account by the regulator to make sure that ICT complies with universal, equal, free and secret suffrage and other relevant conditions. For the case when principles conflict with each other and cannot be fully implemented simultaneously (e.g. when there is a conflict between secrecy of the vote on one side and verification of voting rights on the other), a balanced solution needs to be found, which respects the essence of principles. The decision about such a balanced solution needs to be taken by the legislator and cannot be left to the technical implementation. Whether the decision taking can be delegated to the government, or the CEC should be discussed. In case of delegation, this should be clearly delimitated.

The CoE Recommendation offers detailed examples of requirements derived from the higher-level principles some of which are mentioned below. They apply to e-voting and e-counting. However, they can also offer guidance when considering regulation of other ICT, such as voter authentication and registration, results management, etc.

Universal suffrage requires that the voting interface is understandable and usable by as many voters as possible. Usually, the end-users are involved in the design of the system. The user interface is important. Instructions shall be clear, easy to understand and to follow by as many voters as possible. Consideration must be given to constraints linked to age, language, etc. Furthermore, the specific needs of the disabled should be considered.

Equal suffrage requires that the same information and the same voting options are presented equally on all voting channels, however achieving equality in the way information is displayed is a challenge. Other requirements that aim at ensuring equal suffrage include aggregation of results from all channels; unique identification of voters and measures to prevent double voting by using the same channel or by using different channels to vote multiple times.

Free suffrage requires that the voter's intention is respected, which is particularly challenging when the internet is used to carry the vote or when a "black-box" voting machine, i.e. some form of e-voting without verifiability, is used in the polling station. Free suffrage requires the system to present an authentic ballot, to guide the voter throughout the process, to avoid that he/she votes precipitately, to advise the voter if he/she casts an invalid vote and to inform him/her about the successful completion of the voting. The concept of the chain of trust and the related E2EV requirements mentioned above (cast-as-intended, recorded-as-cast and tallied-as-recorded) aim at ensuring the free suffrage. So does a well-designed use of VVPAT.

Secret suffrage applies throughout the voting process. Encryption of votes and generally of sensitive information that is transmitted e.g. via the internet, separation of voter's identity from the vote, data minimisation (processing and storing only the strict minimum data without which the process cannot be conducted correctly), requirements for identification and authentication aim at ensuring confidentiality. Data protection requirements apply in particular to registers. Secrecy covers also previous choices which have been deleted and replaced. The voter should have the possibility, during e-voting, to cancel a choice and opt for a new one before finally confirming his/her vote. An important requirement is that an e-voting system is not allowed to establish and publish intermediary results before the end of the voting period. Information about participation is of course possible during the voting period. Another requirement is that an e-voting system shall not provide the voter with proof of content of the vote cast, for use by third parties. This attempts to solve the contradiction between providing proof of the vote for voter verification and the prohibition of issuing proof of the content of the vote which can be used to sell the vote or to prove his/her vote to e.g. a coercer. When proof is provided by the system for verification purposes, in the controlled environment at the polling station, procedural measures should make sure that it cannot be used to validly prove the content of the vote to somebody outside the polling station. Secrecy also implies the strict separation between the system used to identify the voter and register his/her participation and the system used for e-voting.

In addition to *data protection*, *information security* and *transparency* are some other aspects which should be considered when envisaging voter authentication, voter registration or results' management ICT, in the light of both national legislation and international (above mentioned) instruments ratified by Georgia.

4.3 Gradual introduction

Step-by-step introduction of e-voting and e-counting is considered a good practice by the Council of Europe and is part of its recommendations in CM/Rec(2017)5. Experts suggest starting with a proof of concept, followed by small scale limited tests (pilots) and their evaluation over the course of several elections. Such experience and its evaluation will provide the ground for deciding on a possible complete roll-out of the solution or not. While these and other suggestions in the recommendation apply specifically to e-voting and e-counting, they may be considered when envisaging other ICT solutions as well.

The trial or pilot period will gauge the solution itself, its capacity to handle all specific situations, its accuracy, usability, accessibility with respect to users with special needs, etc. Other aspects to be evaluated during the testing include the ecosystem in which the solution operates, the human and technical resources required for its setup, use, maintenance, development, etc, and the capacities of the election administration to effectively use the solution and handle possible complications (incidents etc.), financial constraints, etc. The interoperability with other solutions and its integration in the existing architecture, its impact on the planning of electoral processes is tested too.

The trial should be accompanied and followed by evaluations. Evaluation should ideally cover all novelties brought by the solution, including legal, organisational and technical ones. The evaluators may examine the accuracy of results produced by the solution, its security, cost-effectiveness and efficiency, sustainability, the flexibility of the technology to adapt to evolving election regulations, the service provided to the users and their trust in the new technology, etc.

4.4 Stakeholders involvement

Stakeholders' involvement is important. Political stakeholders and ideally the public should be involved in elaborating the strategy that decides on the development of ICT in elections. The main directions should be approved by a large political consensus. Final users, namely voters, in particular those with special needs, need to be involved in the design of the solution. The testing, including invitations to hack the solution, should be open to as many stakeholders as possible, namely the youth, experts, researchers, etc. Finally, stakeholders should also take part in regular audits of the solution that need to be organised periodically.

4.5 Trials phase

The trial phase starts with a proof of concept. Once a satisfactory solution is found, this is then tested during several elections, on a small scale, before being eventually accepted for rollout, reframed or discarded. Tests should take place under realistic conditions.

The duration of the trial, its regulation and the conditions for its evaluation should be foreseen in the initial strategy. Adjustments may be required during the trial phase already. In some cases, prolonging the trial phase may be necessary.

An example of continued prolonging of the trial phase is the introduction of internet voting in Switzerland. It started with regulation introduced in 2002-2003 and first trials in 2004 and has continued in a step-by-step and very cautious way. Several evaluations have taken place, including evaluation reports by the federal government and scientific evaluations. An attempt to introduce legal regulation for a complete rollout started in 2017 but eventually failed to be accepted, namely after problems were discovered thanks to publication of the source code and a public intrusion test which took place in 2019.[24] A discussion with technical was organised in 2020 and informed a new proposal by the federal government for a revised regulation and the prolonging of the trial period. The proposal, currently in consultation, is to re-start a new phase of limited and authorized use of internet voting (for maximum up to 30% of the cantonal electorate) during which only systems that offer complete verifiability will be allowed. The consultation of stakeholders will last some three months before a final decision on the new regulation is taken.[25] This continued prolonging of limited trials reflects scientific consensus

[24] Ardita Driza Maurer, *The Swiss Post/Scytl Transparency Exercise and Its Possible Impact on Internet Voting Regulation*, in R. Krimmer et al. (Eds.): E-Vote-ID 2019, LNCS 11759, pp. 83–99, 2019

[25] On 28 April 2021, the federal Chancellery informed about the opening of a consultation procedure for the redesign of electronic voting trials. The regulatory instruments, namely the Ordinance on Political Rights will undergo a partial revision and the Federal Chancellery Ordinance on Electronic Voting will be completely

that internet voting does not yet offer all the guarantees needed. At the same time, it responds to demands by cantons and other stakeholders, namely the expatriates and the sight impaired, to continue working and developing such solutions to accommodate the needs of special groups of electors.

4.6 Evaluation of tests and decision taking

Evaluation of tests is necessary for deciding on the future use, or not, of the solution. The evaluation should cover legal, technical and social aspects. The main criteria for the evaluation and the moment when it intervenes should ideally be foreseen in the regulation of the trial period. Both benefits and downsides need to be assessed.

Based on the evaluation, the competent authority, most probably the one that approved the strategy and the main directions of development of ICT in elections, needs to decide about a future use and development of the ICT solution or to stop using it. If the experience is evaluated positively and the decision is to keep and further develop the ICT solution, existing regulation of the tests' period should be updated, respectively detailed new regulation should be introduced in line with the requirements of the legality principle.

5 Detailed regulation

Below we consider some elements of the legal regulation of ICT solutions used in elections.

5.1 In praise of detailed regulation

The constitutional principles of universal, equal, secret, free and direct elections grew organically during the nineteenth century, when democracy based on universal citizen participation as we know it today started, and developed in the twentieth century, when paper voting in polling stations and, in some places, open assembly voting (e.g. by raising hand) were the main techniques to express the vote.

revised. This is intended to create a new, stable basis for e-voting trials in which maximum of 30% of eligible voters per canton and a maximum of 10% nationwide may participate. See https://www.bk.admin.ch/bk/en/home/dokumentation/medienmitteilungen.msg-id-83257.html

The requirements for democratic elections that apply today (see Venice Commission's Codes of good practice on elections and on referendums) are based on the interpretation of the principles in the light of the technique used (paper ballot, polling station voting booth, etc.). Interpretation of the principles relies on a good understanding of the technique employed in the specific process. Low-tech techniques like paper, or even mechanical voting, can be understood and evaluated by the layperson. When it comes to digital technologies, this is no longer true. So, one of the first aims of detailed regulation is to spell out the requirements, based on the interpretation of the principles in the light of the envisaged technology. Main requirements should be defined by the legislator or regulator and not left to the technical staff or the solution provider. This ensures a democratic regulation of ICT solutions.

Introducing detailed regulation of ICT involves several steps. The first is to identify the applicable principles and their meaning. Another is to ensure the correct and exhaustive translation of legal principles into requirements for the technology. Finally, there is the question of making sure that the technical solution effectively implements and respects the requirements and, ultimately, the principles.

Clearly identifying the principles for democratic elections that apply to a specific electoral process, in which an ICT solution is expected to be used, is not straightforward. It is sometime subject to legal interpretation. In its judgement of 3 March 2009, which put *de facto* an end to the use of e-voting machines in polling stations in the country,[26] the German Constitutional Court deduced from other constitutional provisions, a principle saying that it must be possible for any citizen, without specialist knowledge and without experts' help, to check reliably the essential steps of the act of voting and of the ascertainment of the results. The regulation of e-voting machines was expected to explain how the voter could do this. As the existing regulation, drafted by the government, did not provide such detailed information (and could not/cannot in the current state of technical development and knowledge), the lower level detailed regulation of EVMs was considered unconstitutional.

Another reason for involving the legislator in the drafting of the detailed regulation of ICT is the situation where it is necessary to find a balanced solution between conflicting principles. In

[26] BVerfGE 123, 39

several electoral processes, no solution (be it low- or high-tech) can ensure 100% compliance with all principles because some of them are conflicting. This is the case for the secrecy of the vote and the necessity to check voting credentials. In such a situation, finding a balanced solution which respects the essence of the principles involves important choices and therefore, such a decision should be taken preferably by the legislator and not be left to the regulator alone, or, even less, to technical experts or to the solution provider.

A second question relates to the correct and complete translation of legal principles into requirements that apply to the technology envisaged. Introducing such regulation requires interdisciplinary competences. Mutual understanding and cooperation between legal, IT and social science specialists is required. This is increasingly important as digital technologies and related security measures become more sophisticated.

One general issue when it comes to detailed regulation of digital technologies relates to ensuring that detailed requirements reflect good practice and state-of-the-art over time. This is relevant for the technical aspects. Detailed requirements that are in line with state-of-the-art are expected to best ensure compliance with democratic principles. However, it is to be noted that state-of-the-art in the digital field evolves rather quickly. Detailed provisions may require frequent updates. The regulatory level of the detailed provision should allow for such frequent updates.

To summarize, compliance of ICT solutions with democratic principles for elections requires legal analysis of the exact meaning of the principles when applied to the specific electoral process. Furthermore, principles should be "translated" into detailed requirements that govern the technology envisaged, including requirements about its control. Combined legal and technical expertise is necessary when designing the detailed regulation. Major decisions, such as those on the scope and the exact meaning of principles or the financial implications of security, must receive broad political backing and are best regulated by the legislator (parliament). Technical choices must reflect good practices and other recommendations of the scientific community (peers). Given the rapid changes in digital technology, an important aspect is ensuring compliance over time. Detailed provisions may need to evolve to reflect the evolution of state of the art and good practices. They are better regulated in lower level regulations. In conclusion, if handled correctly, regulation contributes to clarifying and ensuring compliance of the ICT solution with democratic principles. Below are some detailed requirements that need to be included in the regulation of ICT solutions.

5.2 Functionalities

The regulation should spell out the *functionalities* that the ICT solution is expected to offer. When, for instance, e-voting in polling station is envisaged, regulation should describe the requirements ensuring that the system can handle all possible types of ballots used in elections in the country.

5.3 Usability

The interface with the user is important as he/she should be able to read and execute instructions relatively easily. Consideration must be given to *accessibility* and *usability* questions, namely constraints linked to age, language, etc. Instructions shall be clear, easy to understand and to follow by as many users as possible.

5.4 Secrecy/confidentiality

Data minimisation and data protection are important for election related solutions. Some electoral data, namely the vote, are secret. Detailed and specific requirements on data *secrecy* or *confidentiality* should be foreseen in the electoral legislation and detailed regulation.

5.5 Verifiability

Especially when e-voting and e-counting are considered, requirements related to *verifiability* of the results should be considered. E2EV aims at creating a chain of trust in the e-enabled voting and counting and addresses concerns related to software malfunctioning and to other internal and external threats and risks. If an electronic voting machine is considered, detailed regulation of the voter verified paper audit trail procedure (VVPAT) must be discussed. Most countries that use EVMs are aligning regulations and practices by introducing VVPAT. Paper ballots produced by the VVPAT allow the voter to control the content of her vote before casting it and enable post-election audits that provide confidence in the correctness of the voting results. Regulation should address the question of the respective legal value of the VVPAT and of its counterpart, the electronically registered vote. Informing and sensitising electors on how to make use of the VVPAT is crucial for the VVPAT to effectively play its role and needs to be foreseen. E-counting of hand marked paper ballots is a more broadly accepted and used technology.

5.6 Controls

The regulation should include requirements for controlling the envisaged digital solution and for independently verifying both the solution and the results delivered by it. Controls aim at making sure that the ICT system and its implementation during a specific election comply with requirements.

Controls should take place periodically. Before EVMs or e-counting machines are introduced and after each significant change, formal certification by an accredited, independent and competent body, should be considered. Independent and competent bodies are necessary. After an election, audits that examine the results may be required. Depending on the solution, other forms of control such as intrusion tests, ethical hacking, etc. may be foreseen.

5.7 Transparency

Transparency has several aspects which need to be considered. One of them was mentioned before: the authorities should involve stakeholders and inform broadly about their strategy on introducing ICT solutions in elections. A second aspect relates to the transparency of the solution itself: relevant documents need to be disclosed for verification purposes, at least. We refer to it as "security by transparency". This approach is opposed to "security by obscurity" which is followed by so called black-box systems which are not open for independent evaluation. In certain cases, namely in the internet voting context, this approach has led to public disclosure of relevant system documents, including solution's source code and different audits' and certification reports. This approach seems to gradually impose itself in the internet voting context. A third aspect is transparency about how the solution is implemented and operated during its actual use, e.g. on voting day. This relates to allowing observers to conduct meaningful observation of ICT solutions. In addition to ensuring effective access to the ICT solution, transparency also requires the authorities to contribute to capacity-building of observers and other interested stakeholders interested in making sure that the solution yields correct results.

The mentioned organization of the source code publication and of the public intrusion test of the Swiss Post/Scytl internet voting system in 2019, is a good practice and so far, to our knowledge, the most complete transparency exercise worldwide on an internet voting system used for political elections. Source code transparency in Switzerland was inspired by previous publication of the source code of the internet voting system by Norway, which set the standard for such publication in the e-voting context. Since then, the Estonian and the Geneva internet voting systems have disclosed their source code on GitHub and so does the Swiss Post system. Now, such transparency measures are gaining momentum also with respect to other ICT solutions used in elections.

Another interesting example of transparency related to use of voting machines in polling stations, is the Belgian example. Belgium[27] has set up a "*Collège d'experts*" which has the responsibility of controlling the e-voting system, the establishment of the results as well as any other software used in the specific election also in relation to paper-based voting.[28] The Collège is the only authority legally competent to conduct certain controls. For others, their controlling tasks are complementary to the ones exercised by electoral commissions' staff. Experts keep track of relevant changes in legislation and ensure that external providers integrate them in the e-voting system and other software. The Collège oversees all ICT systems, from different providers and ensures that they interoperate successfully. It organises (conducts, outsources, etc.) controls of the systems before elections, on election day and after elections. Experts register and analyse incidents and draw conclusions and recommendations which apply to the next electoral event. After the election, they publish the source code of main applications.

With respect to transparency of Election Management Systems, a recent OSCE/ODIHR Election Expert Team Report on the Parliamentary Elections that took place in Lithuania on 11 and 25 Oct. 2020, examined the Election Information System used by the Lithuanian CEC which consists of integrated subsystems and modules that support most aspects of the electoral process. These were evaluated against CM/Rec(2017)5 and related Guidelines. The report concluded that to enhance transparency and public confidence, the authorities should publicly test the IT system and publish test and risk-assessment reports before every election. They could also consider making publicly available the source code of its software.

[27] https://elections.fgov.be

[28] See their report of the last 2019 simultaneous elections of European Parliament, national parliament and regional and local legislature https://elections.fgov.be/sites/default/files/inline-files/rapport2019-fr-final.pdf

5.8 Public authorities' and private sector's roles

Public-private cooperation is important when envisaging use of new technologies in elections. However private and public sector's guiding interests are not the same. It is hence important that regulation first, followed by procurement conditions and contractual agreements, clarify requirements, controls and responsibilities. When introducing e-voting for instance, public authorities in charge should make sure that procurement conditions include requirements that are important for compliance of systems and solutions with all applicable legal principles.

Ultimate political responsibility for the conduct of the election should lie with the public authority in charge of elections and cannot be delegated to the solution provider.

5.9 Risk management policy framework

With increased transparency and extended use of ICT, especially of web facing solutions, also come new vulnerabilities and threats. These evolve over time. Despite all precautions, there are remaining risks which need to be addressed. Regulation should foresee a risk management policy framework. The risks of having ICT-backed processes disrupted or otherwise influenced by external unauthorized interventions should be considered. This concerns not only e-voting but also other ICT solutions like registers, public election websites, vote tabulation and counting systems, results reporting systems, auditing systems, etc. which are important for the overall conduct of the election. Cooperation of CEC with e-government and other bodies in charge of information security[29] or cybersecurity is strongly recommended.

Risk analysis and risk mitigation measures should be integral part of the development of ICT solutions. Identified vulnerabilities of the US organisation of elections and their alleged exploitation by a foreign government during the 2016 presidential election are a good case study of what could go wrong with ICT solutions that support the election;[30] work to address them

[29] https://matsne.gov.ge/en/document/view/1679424?publication=3

[30] See e.g. Report of the select committee on intelligence - United States Senate – on Russian active measures, campaigns and interference in the 2016 U.S. election, Volume 1 to 5

may provide useful insights into how such solutions could be better regulated and implemented.[31]

5.10 Disputes and remedies

Regulation should consider dispute resolution mechanisms and remedies such as recounts in the light of the technical specificities of the ICT solutions considered. These probably affect the dispute resolution process (proof requirements, redress options, etc.). The impartial and efficient handling of legal disputes may become even more difficult because traditional measures for detecting errors, namely visual observation, are less important or are even meaningless when ICT solutions are used. The machine is a black box to the voter if no adequate verification possibilities are made available. New possibilities of verification offered to voters and other stakeholders (individual and universal verifiability) as well as remaining risks need to be considered. The possibility that the solution malfunctions should be envisaged and dealt with. General articles in the Criminal Code (e.g. on hinderances to the free participation in elections, forgery of election or of voting results, voting more than once and impersonation, breaching the confidentiality of the ballot) that can be invoked to address ICT related violations may require further development.

When it comes to e-voting and e-counting, recounting is the legal mean for addressing some claims about the results. However, a simple re-count does not make sense if the same machine or software is used, as it will always count the same. Therefore, introducing VVPAT and thus having a paper ballot even when using e-voting in polling stations is necessary. Post-election audits should be foreseen. They use paper ballots. In case of e-counting of paper ballots, the presence of paper ballots makes the audit or recount possible.

In an Election Expert Team report of 8 Feb. 2021 on the parliamentary elections of 11 and 25 Oct. 2020 in Lithuania, OSCE/ODIHR recommends the law to be amended to prescribe means for a recount that are independent of the vote counting software and are based on a randomly selected and statistically meaningful percentage of votes or a number of polling stations.

[31] See e.g. Michigan Election Security Advisory Commission, Report and recommendations, October 2020

5.11 Incidents and communication

The Recommendation notes that where incidents that could threaten the integrity of the system occur, those responsible for operating the equipment shall immediately inform the electoral management body. The competent entity should make sure that the necessary measures are taken, and all interested stakeholders, namely political parties and voters are properly informed.

The main steps that should be taken by the competent electoral authorities to mitigate the effects of the incident should be foreseen beforehand.

5.12 Continued evaluation

Given the evolving nature of the ICT as well as changes in electoral legislation which may affect the organisations of elections, it seems important that ICT solutions are periodically evaluated to make sure that they continue to fulfil the requirements and to respect the principles.

5.13 Sustainability

Sustainable use of ICT solutions in electoral processes refers to several aspects. One is the electoral cycle approach. ICT solutions should consider the degree of automation of the entire cycle. Potential synergies with other low-, or high-tech solutions need to be examined. The lifespan of solutions and its relation to the duration of electoral processes and cycles is an issue.[32] The cycle implies that its processes are reiterated election after election.

Another aspect are costs. They may be excessively high, especially of EVMs and especially in the short term and include not only the cost of purchasing equipment but also operational and maintenance costs, namely those dedicated to maintaining an e-voting system that is state-of-the-art. A lot depends on the technology option that is chosen, but also on the broader strategy and optimization of ICT-related investments.

[32] The purpose of the electoral cycle was to illustrate the fact that elections are not events but processes, and to mainstream this knowledge throughout the planning and implementation of all electoral projects, aiming at longer term commitments of funds and other resources as well as impact beyond the immediate election event. See https://www.idea.int/data-tools/tools/online-electoral-cycle

Digital solutions may improve electoral processes; however, they may also increase complexity. For instance, the planning of electoral cycles becomes more complex and the reliance on solutions provided by (often foreign) vendors increases. So do costs, especially those related to the security of such solutions. Cybersecurity is an important challenge. It is crucial to monitor the resilience of digital systems to cyber threats in order to prevent undue interference or fraud in elections. This means that digital solutions should be regularly updated and trained, skilled staff should be available. This may lead to a situation in which ever greater financial and human resources are required to maintain a constitutionally acceptable election environment, especially for digital solutions accessible via the internet. The overall costs of digital solutions should be considered.

Sustainability considerations have pushed some jurisdictions, e.g. in the USA, to envisage the development of open-source or publicly-owned voting systems that use commercial off-the shelf (COTS) hardware in an effort to reduce both the initial cost and ongoing software maintenance costs associated with proprietary systems.[33] Publicly owned systems require important in-house (within the public institution) capacities and longer term development and funding strategies. Elsewhere, public-private-partnerships (PPPs) are considered more efficient than publicly owned systems. Such decisions should be ultimately validated by the legislator or regulator and should be reflected in the detailed regulation.

Attention should be paid to streamlining election ICT with other strategical developments like online administration, security and other standards development, etc. Building in-house capacities is important, in all cases. Aligning legislation and regulation of EVMs with that of other relevant areas (information security, data protection, critical infrastructure, etc.) and with international recommendations is important.

5.14 Information and training

Another important challenge is the effective use of ICT by staff, voters, observers, media, etc. It is not enough to elaborate technically secure solutions. They should also be correctly used and understood. This points to the need to inform and instruct voters and other users that interact

[33] See “Securing the vote. Protecting American democracy – A consensus study report of the National Academies of sciences, engineering, medicine”, 2018

with the ICT solutions. Achieving this requires continued efforts. Gradual introduction is therefore necessary also for allowing for the upskilling and information of all stakeholders, which are necessary for the successful use of the solution.

5.15 Public trust

Trust relates mainly to perceived trust and to the trustworthiness of the solution. Regulation addresses both. Trust has another aspect: often introducing ICT is seen as a solution to the issue of lack of trust in the existing electoral administration. This perspective is questionable.

One main way to instil the perception trust is transparency. Involving stakeholders in elaborating the strategy for ICT in elections, cooperating with experts, involving the public (hackers, students, experts etc.) in testing the e-voting system are good practices that can instil trust that the authority handles ICT correctly.

Regulation needs to clarify that only trustworthy solutions are introduced. Cooperation with research helps identifying solutions which can be considered trustworthy. Often legal requirements refer to state-of-the-art solutions. Attention should be paid to the fact that state-of-the-art may evolve quickly and thus regulation and the ICT system should be capable of being upgraded and of evolving.

With respect to the frequently invoked argument of introducing ICT in order to increase trust in the voting process, there is consensus in the CoE region, as pointed out in CM/Rec(2017)5, that trust in the electoral system and the electoral authority is *a precondition* to the introduction of ICT in elections. The electoral authority has a major role to play in regulating, planning, introducing, supervising and controlling e-voting and other ICT solutions. If the authority is not trusted, the ICT solution will not be trusted either.[34] One way to gain trust is to conduct broad consultations before e-voting is introduced, to follow good practice and recommendations, proceed gradually, cooperate with research, provide information, training, transparency, etc. If

[34] In their conclusions of the observation of PE of 2017, PACE stresses this point by saying that new technologies are welcome in electoral processes, but they must never be considered as a substitute for trust. See: https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=23748&lang=en

not supported by broad consensus, introduction of ICT may even produce the opposite effect, i.e. decrease trust.

6 Recommendations

The following are general recommendations. They apply fully to e-voting in polling stations or e-counting. To a certain extent only, they apply to voter authentication and registration solutions which are less complex and easier to protect.

1. Inform and involve stakeholders in thinking out the future use of ICT in elections.
2. Define the main directions of development.
3. Identify the needs and the expectations.
4. Conduct feasibility study/ies.
5. Elaborate a strategy and be transparent about it.
6. Introduce regulation of the testing phase. Involve IT, legal and social science research.
7. Procure and approve a prototype.
8. Conduct small scale trials, starting with lower level elections.
9. Evaluate the trial phase based on well-defined criteria.
10. Decide about the future: redesign and/or extend trials; complete rollout; abandon.

If, after the piloting phase, the decision is taken to pursue the use and development of the ICT solution/s, then it is recommended to:

11. Clarify the application of principles (possible changes in the law).
12. Introduce detailed regulation for the extended trials or the complete rollout of the ICT solution. Involve IT, legal and social science research.
13. Procure and approve the ICT solution.
14. Regulation should address the functionalities, the usability, secrecy or confidentiality, verifiability, evaluation including certification of the solution, transparency, the role of public authorities and of private sector providers.
15. Despite all due care, there are remaining risks when ICT is involved. These should be addressed in a risk management policy framework.
16. Dispute regulation elements (proof, remedies, etc.) should be re-considered in the light of possibilities and limitations of the ICT.

17. Address measures to be taken in case of incidents, including information and communication ones.
18. Conduct regular evaluations of the ICT solution to confirm its constitutional compliance as ICT related risks evolve and electoral law changes.
19. Evaluate sustainability.
20. Periodically inform and train the public and stakeholders. Do so especially before an election
21. Be transparent about all aspects of the use of ICT to instil trust in that specific solution and in the system in general. Require that only state of the art ICT solutions are used.
22. Trust in the electoral administration is a prerequisite to the use of ICT in elections.