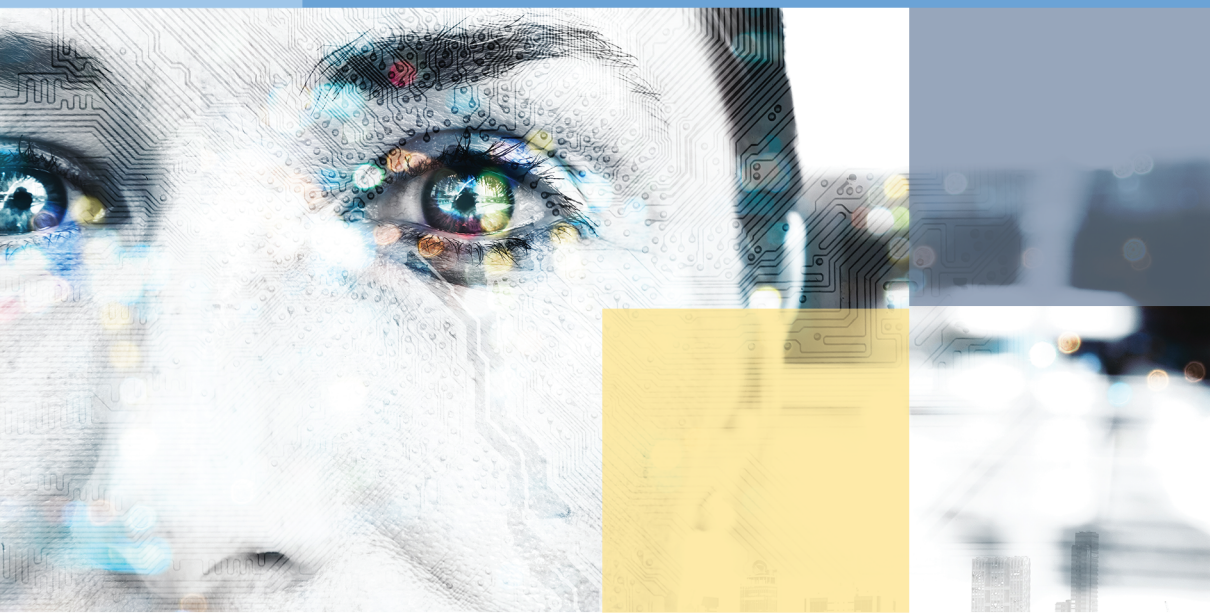
DIGITAL TECHNOLOGIES IN ELECTIONS

Questions, lessons learned, perspectives



COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

DIGITAL TECHNOLOGIES IN ELECTIONS

Questions, lessons learned, perspectives

Ardita Driza Maurer

Council of Europe

This publication is developed by the Division of Elections and Civil Society of the Council of Europe within the framework of the Council of Europe project on "Supporting the transparency, inclusiveness and integrity of electoral practice in Ukraine".

This publication contains original unpublished work. The opinions expressed herein belong to the author and do not necessarily reflect the official position of the Council of Europe.

Design and layout:
Ganna Vojna

Cover photo: Shutterstock

Council of Europe Publishing
F-67075 Strasbourg Cedex
http://book.coe.int

Printed at the Council of Europe

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

ELECLAB

URSO
Useful
Relevant
Sustainable
Owned

Developing a regulatory framework for digital technologies used in the electoral cycle*

* This study was conducted upon the request of the Central Election Commission of Ukraine with the support of the Council of Europe project on "Supporting the transparency, inclusiveness and integrity of electoral practice in Ukraine", implemented within the framework of the Council of Europe Action Plan for Ukraine 2018–2021.

Content

INTRODUCTION

Digital solutions are already used in different phases of the electoral cycle by election management bodies (EMBs), voters, political parties, electoral justice, media, and others. Geographic information systems for boundary delimitation and establishing the location of polling stations, electronic voters' registers, electronic voting machines or internet voting systems, optical scanners that count paper ballots, e-solutions to transmit election results from polling stations to central authorities, e-signing of initiative or referendum demands, e-signing of lists of candidates or party endorsement, systems for the consolidation and publication of results or their visualisation by geographic areas, statistical methods to evaluate the accuracy of results and detect potential fraud are some examples of digital solutions used in the electoral cycle. They are based on digitised information. Other digital technologies used or envisaged include biometry, blockchain, cloud computing, artificial intelligence, etc.

Digital solutions for elections must comply with the applicable principles for democratic elections. However, the practical application of legal principles to digital technologies is not easy. The first difficulty lies in the general character of legal principles which are formulated in general and broad terms. Their application to a specific context requires interpretation which must clarify the exact meaning and practical implications that arise from the principles. The second major difficulty lies in the technical nature of digital solutions, whose internal setup and functioning can be understood only by a handful of specialists but not by the layperson without technical help. Yet, it is the layperson (voter, election administrator, judge, observers, etc.) who must use, check and ultimately trust the digital solution and the results it yields.

Regulating the use of digital solutions means roughly two things. In the first instance, it is necessary to concretise the principles for democratic elections, namely to clarify their meaning and extract the requirements that apply to the respective context. The second step is to translate these legal requirements into provisions that regulate the setup, use and control of the digital solution. Regulation should ensure that the use of digital solutions is regulated sufficiently to guarantee the respect of the higher-level principles.

Regulation is important for those who build digital solutions, those who decide to introduce them, those who use, monitor, and control them, etc. This could be the polling station worker, the voter, observers, the central administration of voting results, etc. It is therefore important to have a good regulatory framework so that the rights, obligations, competences, etc. of all those involved are clear to

them. Ultimately, regulation is important to ensure that elections are free, fair, and democratic.

The Council of Europe and its member states have discussed the use of digital technologies in elections for the past twenty years. E-voting and e-counting have been the focus of this attention. The Council of Europe adopted the first recommendation on e-voting in 2004 and updated it in 2017,[1] extending the definition of e-voting to also include the e-counting of paper ballots. However, other digital solutions used during the electoral cycle, such as e-registers, solutions for voter information, vote tabulation, results transmission, etc. are not covered by the Recommendation of the Council of Europe Committee of Ministers CM/Rec(2017)5 on standards for e-voting.

In the following paragraphs, we present an overview of relevant international legal instruments and some questions that the legislator or regulator should consider when faced with the introduction of digital solutions in elections. The focus is on guiding principles, good practices, and lessons learned.

Two preliminary remarks: firstly, electoral and political processes are country specific and influenced by historical, geographical, cultural and other specificities. This means that a solution found to be successful in one place may not be implemented in the same way and/or may not be successful elsewhere. However, digital solutions also share common technical characteristics, independently of the context. This paper focuses on these common features and, as such, the general conclusions presented here should be valid in all places.

Secondly, existing guidance on e-voting may apply to other digital solutions used in elections, voting being the most complex and sensitive step in an election. Indeed, this paper will often refer to experiences of e-voting. However, this paper brings a few novelties, compared to existing documents on e-voting: it considers all digital solutions and is not limited to e-voting and, furthermore, it also includes some lessons learned from recent experiences in e-voting, namely on transparency and verification, which have not yet been reflected in e-voting guiding instruments. To be noted, the Council of Europe is currently working on possible guidance on the use of digital technologies in elections in line with the conventional principles for democratic elections.[2]

1. Previous Recommendation of the Committee of Ministers of the Council of Europe Rec(2004)11 on legal, operational and technical standards for e-voting and the associated Guidelines on certification and transparency. They were replaced by the Recommendation CM/Rec(2017)5 on standards for e-voting and the associated implementation Guidelines.

2. See work by the Council of Europe/European Committee on Democracy and Governance (CDDG) on guidance on the use of digital technologies throughout the electoral cycle, except the voting phase, which is already addressed by the Recommendation of the Committee of Ministers of the Council of Europe CM/Rec(2017)5, electoral campaigning (social media, information, disinformation) and financing issues which are addressed by other initiatives.

LEGAL STANDARDS

This contribution focuses on the application of the principles of free and fair democratic elections. Other election-relevant principles, such as freedom of opinion and expression, freedom of peaceful assembly, freedom of association, freedom of movement, freedom from discrimination, the right to an effective legal remedy need to be considered, too. However, they will not be discussed here.

International and national instruments that regulate elections as well as digital technologies are relevant when considering regulating the digital solutions used in elections.

1. Legal framework for elections

a. International instruments

Binding international law includes Article 21 of the 1948 United Nations Universal Declaration of Human Rights (UDHR),[3] Article 25 of the 1966 UN International Covenant on Civil and Political Rights (hereinafter – ICCPR) and Article 3 of Protocol №1 to the Convention for the Protection of Human Rights and Fundamental Freedoms (hereinafter – Article 3 of Protocol № 1 to the Convention) as interpreted by the European Court of Human Rights. These instruments are binding in the countries that have ratified them.[4] The Charter of Fundamental Rights of the European Union contains similar rights and applies to EU countries.

Authoritative interpretations of the above-mentioned instruments, other political commitments, and principles of the so-called European electoral heritage are equally part of the international legal framework for elections. This includes, in particular, the ICCPR's General Comment 25, the case law of the European Court of Human Rights on Article 3 of Protocol № 1 to the Convention, the 1990 Copenhagen Document of the Conference for Security and Co-operation in Europe (CSCE) and other election-related commitments, 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.

Authoritative studies and evaluations of elections and of regulatory frameworks for elections also offer guidance, provided due account is taken of the particularities of

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

4. All Council of Europe member states have ratified the UN International Covenant on Civil and Political Rights; some have introduced reservations (for example, Switzerland on vote secrecy/Article 25 ICCPR). 45 out of 47 Council of Europe member states have ratified Protocol № 1 to the Convention. Switzerland and Monaco have signed but not ratified it so far. However, with the exception of the lack of secrecy, an accepted feature of assembly voting in Switzerland (voting by raising hands), all other elements of Swiss law are stricter and broader compared to Article 3 of Protocol № 1 to the Convention. This is usually so in other countries as well. International provisions usually offer minimum standards which are respected and exceeded by national laws.

the case that is being evaluated and the extent to which the recommendations can apply elsewhere. For instance, the election monitoring reports of the OSCE/ODIHR (Office for Democratic Institutions and Human Rights of the Organisation for Security and Co-operation in Europe), PACE (Parliamentary Assembly of the Council of Europe) etc., and joint OSCE/ODIHR – Venice Commission evaluations of electoral regulatory frameworks, in particular, those that address the use of digital technologies in elections, are of interest. Other studies, such as the OSCE/ODIHR 2013 Guidelines for reviewing a legal framework for elections, and guidance from the OSCE/ODIHR on observing and evaluating the digital solutions used in elections (including their regulation), are of interest to the regulator. These documents offer valuable hints; however, they do not provide comprehensive guidance on how to regulate the use of digital technologies in elections.

The Council of Europe has done doing pioneering work on the regulation of digital technologies used for voting and counting. It adopted the first recommendation in 2004, which was then replaced by the Recommendation of the Committee of Ministers of the Council of Europe CM/Rec(2017)5 on standards for e-voting. This is the only international instrument which offers guidance on how to translate the principles of the European electoral heritage into requirements for e-voting systems. The principles include universal, equal, free, secret and direct suffrage, the organisation of elections at regular intervals, respect for fundamental rights, regulatory levels and stability of electoral law, and procedural guarantees. The Recommendation CM/Rec(2017)5 contains 49 standards, namely detailed requirements (Appendix 1) that apply to all kinds of e-voting and e-counting. They are explained in the Explanatory Memorandum of the Recommendation. Implementation guidance is to be found in the associated Guidelines for the implementation of the Recommendation CM/Rec(2017)5. Although the recommendation only deals with e-voting and e-counting, its standards may be considered when envisaging other digital solutions.

b. National instruments

The regulation of elections is a national prerogative. Higher level principles governing elections are found in the national Constitution and/or national electoral law. They embrace and develop international principles. Detailed requirements are usually found in lower level regulations. Elections to the European Parliament are additionally governed by the European Act concerning the election of the members of the European Parliament by direct universal suffrage. In some countries, local elections may be regulated at the local level. However, with respect to free and fair democratic elections, all legal frameworks (supranational, national, and local) incorporate at least all higher-level principles of the above-mentioned international instruments (ICCPR and Article 3 of Protocol № 1 to the Convention).

The higher-level principles of democratic elections were gradually introduced in national legislations and practice in the 19th century, when democracy based on citizen participation as we know it today started to develop following the American

and French Revolutions.[5] Technology (low and high) has accompanied these developments. The introduction of the Australian ballot in the mid-19th century came as a reaction to the extension of suffrage rights to masses of voters: open voting was no longer tolerable because it could and did involve undue influence.[6] Mechanical voting machines had already been introduced in the 19th century, followed by electronic computers in the 1960s, the introduction of direct recording electronic voting machines (DREs) in the 1990s and internet voting in the years after 2000.[7] Mechanisation first, then computing technology have accompanied and supported several legal reforms: fighting fraud,[8] promoting voter equality, enfranchisement, efforts to facilitate voting, and efforts to increase participation.

At the national level, there have principally been two waves of regulation regarding the technologies used in elections. Initially, regulations on low-tech (paper and mechanical solutions) were introduced, namely in the 60s and 70s in Germany, the Netherlands, and France. Later, these regulations were "updated" to govern digital solutions, mainly the use of e-voting or e-counting machines in the 1990s. Countries that opted for internet voting developed new dedicated regulations based, however, on analogies with existing paper-based systems, namely postal voting (for example, Switzerland or Estonia, beginning of 2000).

Despite being quite detailed compared to the regulation of paper or mechanical voting, regulations on voting machines in Germany, the Netherlands, and France were found to be in breach of constitutional principles. The benchmark (that which constitutes compliant regulation) is defined by the legislator, the constitutional judge or the regulator and, sometimes, it is not clearly defined. Furthermore, definitions vary. In some countries the benchmark was such that regulations could not be updated and voting machines have subsequently been suspended (Germany, the Netherlands). Elsewhere, the use of voting machines has been drastically reduced (France) as the existing regulation is unsatisfactory. In other countries, regulatory updates introduced significant changes, enabling voting machines to remain in use (Belgium, introduction of VVPAT- voter verified paper audit trail).

Internet voting regulations have evolved even more quickly. In Austria, the regulation was considered to breach the Constitution as it was not detailed enough to enable election commissioners to conduct their tasks without technical assistance. As the said regulation did not and could not be updated to satisfy

5. *Encyclopædia Britannica:* There is a direct relationship between the size of an electorate and the formalization and standardization of its voting practices.

6. *Encyclopædia Britannica:* The Australian ballot, also called the secret ballot, is a system of voting in which voters mark their choices in privacy on uniform ballots printed and distributed by the government or designate their choices by some other secret means. It was introduced initially in Australia and spread to Europe and the United States to meet the growing public and parliamentary demand for the protection of voters.

7. This trend was and is not specific to elections. Since the Industrial Revolution of the late 18th and early 19th centuries, technology has powered growth and transformed economies.

8. Fraud was quite extensive especially in the 19th and first half of the 20th century. In the USA, for instance, where corrupted jurisdictions resisted the introduction of voting machines. See, for example, Douglas W. Jones and Barbara Simon's 2012 *Broken Ballots - Will Your Vote Count?*

the constitutional requirement, so internet voting cannot be envisaged in Austria. In Switzerland, evaluation of the long experimentation phase and of the first-generation regulation introduced in 2002 led to important updates to the regulatory framework in 2013. The second-generation regulation introduces novelties that reflect a better understanding of digital technologies: risk policy, verifiability requirements, extensive controls by independent and expert bodies, stricter data protection and transparency requirements, etc. The Council of Europe recommendation on e-voting followed a similar path and so did Estonian regulation. Recent experiences with the application of the new regulations (Switzerland, Estonia) show that they still need to evolve to better address verifiability or transparency. Such a dynamic is of interest when envisaging the regulation of other digital solutions as well.

Case law in the highest national courts has played an important role in clarifying the practical meaning of electoral principles as applied to digital solutions. Much discussed have been the decisions by Germany's Constitutional Court (2009) or the Austrian one (2011). Case law shows the importance of interpretation in translating principles into detailed requirements for technologies and has helped to build global consensus on the need for detailed regulation of digital technologies. It shows that the same principles can be interpreted in very different ways and lead to different results depending on factual, historical, and cultural specificities. This kind of interpretation should not be left to technicians or providers of technology but should be made by the legislator/regulator.

When compared to e-voting, other uses of digital solutions in elections have been under-regulated so far. However, there is increasing awareness that this should change as they play a role in the integrity of elections. Studies and reports that evaluate the set up and use of digital solutions at a national level are of interest to the regulator.

2. Legal framework for new technologies

a. International instruments

Legal instruments that address digital technologies may be highly relevant although they do not deal specifically with elections. For example, the Convention on Cybercrime of the Council of Europe (Budapest Convention) serves as a guideline for any country developing comprehensive national legislation against cybercrime and as a framework for international co-operation between state parties to this treaty. A guidance note on election interference explains how the Budapest Convention may apply to aspects of election interference by means of computer systems. The Convention on Cybercrime criminalises several types of conduct, namely would-be-crimes directed at elections. Its procedural powers and mutual legal assistance provisions are relevant when investigating and proceeding against election interference.

Data protection instruments, namely the Council of Europe Modernised Convention for the protection of individuals with regard to automatic

processing of personal data (Convention 108+) and the EU reference instrument, Regulation (EU) 2016/679, General Data Protection Regulation (GDPR)[9] are relevant. The Council of Europe Convention 108+ and the GDPR were developed in parallel and are consistent with each other. A European Commission guidance document explains the application of the GDPR in an electoral context. However, most data used in elections are qualified data whose processing can only be allowed if appropriate safeguards are enshrined in law. This means that election-data protection should be covered in election-specific regulations which are more stringent than data protection instruments.

Supranational (EU) legislation on cybersecurity is emerging. Adopted by the European Parliament in July 2016, the Directive on the security of network and information systems (NIS Directive) is the first piece of EU-wide legislation on cybersecurity. It provides legal measures to boost the overall level of cybersecurity in the EU by requiring Member States to be appropriately equipped, setting up a co-operation group to support and facilitate strategic co-operation on cybersecurity incidents and exchange information about risks, and promoting a culture of security across sectors that are vital for the economy and society. Following the Directive, an EU Cybersecurity Act was adopted in 2019 which introduces, for the first time, an EU-wide cybersecurity certification framework for ICT products, services, and processes.

More recently (especially since 2016), emphasis has been placed on the cybersecurity of the digital solutions used in elections and the concrete application of international instruments on data protection or cybersecurity to them. The European Commission has produced guidance on the application of the European Union data protection law (GDPR) in the electoral context.[10] Work at the EU level on the cybersecurity of election technology resulted in a Compendium on Cyber Security of Election Technology which aims at sharing experiences and providing guidance as well as an overview of tools, techniques, and protocols to detect, prevent, and mitigate cyber threats. The Council of Europe Cybercrime Convention Committee (T-CY) has produced guidance on the application of the Budapest Convention to election interference by means of computer systems. Other documents of interest provide an overview of how different countries deal with such issues and identify good practices (e.g. the International Institute for Democracy and Electoral Assistance/IDEA, Cybersecurity in Elections and Models of Interagency Collaboration, 2019).

9. 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.

10. European Commission, Free and fair elections – Guidance document. Commission guidance on the application of Union data protection law in the electoral context. *A contribution from the European Commission to the Leaders' meeting in Salzburg on 19-20 September 2018* (COM(2018) 638 final).

b. National instruments

In a similar way, national laws on data protection, transparency, cybersecurity, e-identity, registers' management, etc. apply to digital solutions used in elections, even if these laws do not specifically address elections, and unless there are specific rule in the electoral legal framework on the same issues (*lex specialis*) which take priority.

National regulations on cybersecurity or protection against cybercrime are being aligned with international instruments. Good practices for the cyber security of election technology are being identified (for instance, the mentioned EU Compendium on Cyber Security of Election Technology, initially published in March 2018) and are expected to contribute towards further harmonising national practice in these areas.

3. Inspiration from other fields

Digitisation impacts all areas of life. It disrupts, by supplanting previous ways of doing and questioning older skills and approaches. Law and other fields are under pressure. It is interesting to observe how other sectors, for instance, critical systems similar to elections, handle the challenge.

A fragmented approach to the applicability of law on the internet, focusing on compliance with data protection, or with cybersecurity, etc. can be observed.[11] In the field of elections, however, it is admitted that stricter standards should apply to all these issues and such standards need to be set in the dedicated electoral regulation. So, in elections, there is a chance that the approach could be less fragmented.

The protection of fundamental rights in the digital context is a common preoccupation. Admittedly, the application of fundamental rights to digital technologies should be strengthened to counter erosion trends. There is no need for new constitutional provisions addressing digital technologies but there is a great need for the effective application of existing constitutional provisions to digital technologies. The big challenge is how to do it. This is indeed the challenge for the legislator when regulating digital solutions in elections.

As an example, we can refer to the health system, which has taken up and makes use of many digital solutions. It is a critical system for society. In many countries, the experience can be summarised as follows: "We have seen a number of DHT [digital health technology] solutions come on to the market in recent years. Some have been good and some not so good, but what we have really struggled with is defining a shared standard of what good looks like".[12] This observation can be made in the electoral field too. The answer should be found in the regulatory framework for digital solutions in elections.

11. Instead of many, see Udo di Fabio, *Grundrechtsgeltung in digitalen Systemen, 2016*

12. UK National Health System, How we assess health apps and digital tools, https://digital.nhs.uk/services/nhs-apps-library/guidance-for-health-app-developers-commissioners-and-assessors/how-we-assess-health-apps-and-digital-tools#top

QUESTIONS FROM AND FOR THE REGULATOR

When envisaging digital solutions to replace, complement or augment the existing low-tech solutions used in elections, the legislator[13] is faced with questions that meet at the crossroads of electoral law and digital technologies. The following ones are based on the reviewed documents (see References below).

1. Problem identification

Digital innovations may be best introduced as a solution to existing problems, not as an end in itself. Clearly identifying the problem that needs to be solved is the first step towards finding an appropriate solution. The "problem" is the difference between the existing situation and the desired one. It may be an identified issue that must be corrected, a potential gain in efficiency, or improving the achievement of higher-level principles.

Identifying the "original" problem is helpful with a view to distinguishing it from subsequent problems that may arise from the use of the digital technology and to weighing up competing rights. Part of the "problem" identification is to identify those affected by it or interested in resolving it and their expectations. These may be the voters (for example, expatriates, sight impaired, etc.), election administration, political competitors, etc. Any innovation in the electoral cycle should take account of the interests present. Proposals for digital solutions should draw on research about the problem and user expectations.

After having identified the problem, and before a solution is chosen, it is necessary to assess the efficiency of existing solutions and of potential ones to achieve free, fair, and democratic elections. It is important that such assessments are broadly shared.

2. Goals and objectives

The next step is to identify the desired situation and set objectives towards that goal. Objectives (quantitative and qualitative ones) will be the evaluation criteria for the solution. The goal and the objectives should be "solution neutral". Experience suggests that one should avoid starting from a clear idea of the solution when defining goals and objectives. Furthermore, the goals and objectives should be consensual.

Based on this, the next step is to identify potential solutions. All possible solutions should be considered with the aim of finding those that better contribute towards strengthening the constitutional principles. Experience shows that digital solutions might not be the best option in all instances. Analysis of their benefits and risks is

13. We use legislator (usually the parliament), or regulator (usually the Government or its units) as synonyms in this paper.

the next important step. For example, a working group from the Ministry of Justice in Finland concluded that online voting should not be introduced in general elections as its risks are greater than its benefits. Although technically feasible, the technology was considered as "not yet at a sufficiently high level to meet all the requirements", referring to the reconciliation of verifiability and secrecy.

3. Benefits and downsides

To assess the opportunity to introduce an envisaged solution, the legislator should consider both its benefits and downsides. Usually, the legislator receives information on these aspects by the initiator of the regulation and may also consult other experts.

Some benefits concern the election administration, others may concern voters or, more generally, the whole system. From the perspective of election administration, digital solutions may provide quicker results, involve a reduced risk of mistakes, facilitate interactions and information sharing in real time or improve controls of registers by providing effective mechanisms for identifying duplicate entries. Efficiency and cost-effectiveness may be outlined. Benefits are not perceived in the same way in different countries. For instance, mobile technology that enables election results to be announced sooner may be considered very beneficial in countries where it helps diffuse tension in closely contested elections, whereas it is considered less crucial in other places with a less conflictual political culture.

From a voter or democratic perspective, digital solutions may offer advantages in terms of availability (online registration, distance voting), independence (for example, some e-voting may offer people with disabilities an opportunity that they might not otherwise have had to vote secretly), by preventing involuntary mistakes in filling in ballots, etc. Introducing technologies for the sake of appearing modern to the electorate is not recommended.

The legislator should be able to get an informed opinion on the real benefits. Some of them can be measured already before introduction (for instance, efficiency, speed, error-freeness, transparency, etc.). Others are more hypothetical and impossible to measure until the solution is effectively in use (for example, increase participation, enhance voter confidence). Given this, the legislator may consider mechanisms for the periodic evaluation of benefits and downsides after the solution is introduced, and periodic reassessment of these solutions.

Significant debate should take place before the decision is taken to introduce digital technology in elections. The main challenges should be openly discussed. The challenges include the sustainable and cost-efficient use of the technology. The relatively high maintenance costs of the machines and updating the software is an issue that has been reported by a number of countries.

Additionally, cybersecurity is emerging as an important challenge. It is crucial to monitor the resilience of these digital systems to cyber threats in order to prevent

undue interference or fraud in elections. Digital solutions should be regularly updated. Trained and skilled staff should be available and on hand. Situations in which ever greater financial and human resources are required to maintain a constitutionally acceptable election environment are possible, in particular, for digital solutions accessible via the internet such as remote voting. The costs of testing the systems on a regular basis or those related to the storage and renewal of equipment or to the need for qualified staff are important elements to take into account.

Technology may help improve electoral processes; however, early embracers of this technology also report greater complexity as a result of introducing ICT. For instance, the planning of electoral cycles becomes more complex. As the costs of organising elections increase, so does the granting of significant contracts to private sector firms, often international ones. Possible dependence on private sector solutions is a major downside that needs to be debated by the legislator.

The impact of potential failures in digital solutions on the integrity of elections is yet another issue of concern. A major negative impact on the electoral cycle may in principle be achieved with relatively little effort by compromising digital solutions. At the same time, innovative solutions may be envisaged that help counter such risks. The legislator should have a good understanding of the benefits, downsides and respective solutions to be able to make meaningful assessments and make good decisions.

As a rule of thumb, to counter shortcomings, it is important to be patient with the introduction of digital solutions. Clear objectives, feasibility studies, and pilots should precede and guide the introduction of digital solutions in the electoral process. We suggest that the periodic evaluation of benefits and downsides after the solution is introduced, and periodic reassessment of these solutions, is necessary.

4. "Electoral cycle" approach

The legislator should think as broadly as possible, in terms of the use of digital solutions throughout the electoral cycle. One initial question, according to experience, is to study the degree of automation in the entire cycle. The ambition is to understand and regulate the use of digital technology throughout the cycle, not just specific solutions. Solutions may evolve rapidly whereas the main features of the underlying technique will very likely persist over the long run and must be regulated for the whole cycle.

Integration of digital solutions and their potential synergy with other low-tech solutions used in the electoral cycle need to be examined. The lifespan of digital technologies is an issue. It may be relatively short and it is necessary to match the lifespans of different technologies used throughout the electoral cycle.

Another important aspect is for the legislator or regulator to review with a critical eye all processes whose digitisation is being considered. It is well

known that technology will not improve the underlying process if the process has problems; digital technology may magnify them and be more detrimental than low tech.

5. Multidisciplinary approach

The legislator should approach the regulation of digital solutions not only with legal arguments and reasoning but also with a good understanding of technical issues. This requires multidisciplinary work. Very important aspects are definitions and interpretations. Definitions are important for mutual understanding and several glossaries have been developed in recent years that explain legal and technical terms to specialists in both fields (examples include Appendix II of the Recommendation CM/Rec(2017)5, Venice Commission glossary of electoral and technical terms, etc.). Such definitions are necessary and important but not sufficient.

Digital solutions are based on mathematics. Programmers need formal/rigid definitions of the relevant legal concepts (for example, principles of free and fair democratic elections) based on which they create models or solutions. If the underlying definitions change, the solution also needs to evolve. In practice, legal principles are defined broadly. Their application to concrete situations requires interpretation. Interpretation will reveal what the meaning of a concept should be in each context. Interpretation is also required to assess conflicting concepts and values. When it comes to digital solutions, it is important that these interpretations are done by the competent authority and are not left to solution providers or technicians alone.

A multidisciplinary approach is necessary. It will require iterative exchanges between legal and technical experts. The legislator must foresee an adequate framework, resources and time for this important dialogue to take place.

6. A sovereign decision

The acceptability of the use of digital solutions in elections depends on their compliance with the higher-level principles, including those of free and fair democratic elections. This compliance is to be ensured first in the regulation.

No international guiding document requires countries, and respectively legislators, to introduce digital technologies in elections. As explained previously, this decision depends on many factors, some of them country specific. Furthermore, digital technology is not always the best solution. The approach of international instruments is to encourage countries to understand that the constitutional conformity of digital solutions must be ensured and propose guidance on doing so. Even when the introduction of digital tools is encouraged, the necessary compliance with the principles of free and fair elections is a strong precondition (e.g. the EU amended Electoral Act (not in force) which gives Member States the freedom to offer … electronic or internet voting, if they are sure to uphold

the relevant EU rules on the protection of personal data, voting secrecy and the reliability of results).[14]

At some point, international decisions may, as a side effect, impose the digitisation of electoral processes on countries. The EU amended Electoral Act (not yet in force) inserts a new article which imposes on each member state the obligation to designate a contact authority responsible for exchanging data on voters and candidates with its counterparts in other member states for the purpose of avoiding multiple entries in registers and multiple voting. Such exchanges impose the de facto digitisation of registers, as it seems impossible to meaningfully achieve the goal of comparing data and identifying double entries if such work is to be done manually. This kind of "forced digitisation" should be thoroughly discussed before it becomes mandatory.

Ultimately, the decision to introduce digital solutions is a national prerogative to be taken by the national legislator based on considerations specific to the national situation. As attested by Germany's Constitutional Court decision of 2009, every society has to find its own solution and consider the broader implications of every modernisation, including its price. Each society, namely legislator, has to decide if it is willing and able to pay that price, which may be a financial one or involve other more important values. The legislator should also decide whether the country is ready and capable of introducing modernisation that is sustainable and beneficial. A good approach is to conduct tests that will provide important information on decision taking.

7. Necessity, form, and level of regulation

Regulation is the founding layer of a constitutionally compliant digital solution. Experience shows that regulation is often considered at the end of the process of introduction, after the solution is almost finalised. This is wrong, as also shown by the previous discussion on problem identification, assessment of goals, and objectives, etc. The regulation is expected to offer guidance on the development of solutions. This means that the legislator should proactively regulate the main aspects of the use of digital technologies in elections, in a solution-neutral way.

As demonstrated by the experience of many countries (USA, Germany, the Netherlands, France, etc.), legacy regulations, inherited from mechanical or other low-tech solutions, are not appropriate for regulating digital solutions, even if they have been upgraded. In general, analogies with traditional processes are not enough. As the German example shows, it is not sufficient for the law to stipulate

14. Article 223 of the Treaty on the Functioning of the European Union, which provides for the amendment of the Electoral Act, does so with the aim of obtaining *"a uniform procedure in all Member States or in accordance with principles common to all Member States"*. In addition to harmonising the substantive rules (for example, different minimum age to stand as a candidate in elections or common minimum thresholds), the act also aims *"to encourage voter participation in elections to the European Parliament and to fully take advantage of the possibilities offered by technological developments."* Article 4a says *"Member States may provide for the possibilities of advance voting, postal voting, and electronic and internet voting, in elections to the European Parliament. Where they do so, they shall adopt measures sufficient to ensure in particular the reliability of the result, the secrecy of the vote, and the protection of personal data in accordance with applicable Union law"*. It is not clear, however, which evidence the authors of the Act used to conclude that e-voting will increase participation.

that "machines may be used provided the secrecy of the vote is guaranteed" (Article 35 of the Federal Election Act). A detailed regulation should clearly indicate what this implies and enable independent controls to make sure that these requirements are respected.

Who regulates what is another question. In some countries, it was the courts who defined how the regulation should look in order for it to be compliant. The German Constitutional Court said that regulation should be detailed to the point of enabling the citizen to control how his/her vote is handled without technical knowledge or support. This is an important definition of transparency in elections. Of course, the German Constitutional Court "uncovered" this definition (based on its interpretation of the relevant constitutional provisions) and did not invent it. In other countries such as the USA or Switzerland, courts have invited the legislator to make these definitions. In India, the highest court decided that a voter-verified paper audit trail is required for voting machines to respect the principles, but its decision had already been anticipated by the electoral authority. The common element in all cases is that the definition of the concrete meaning of higher principles in a context where digital solutions are used affects the very meaning of the principles. So, the decision has to be taken by the competent authority, usually the legislator.

Delegation of regulatory powers to the government, or the central election commission, etc. should be clearly framed. For instance, the Venice Commission and the OSCE/ODIHR have underlined that the use of digital solutions, which are core issues in election procedures (for example, internet voting), has to be defined clearly in law.

Regulatory aspects are more complex in federal states. Implementing new technology in this case must also contend with a decentralised system of administering elections. In Argentina, provinces extended regulatory powers and the discrepancies between provincial regulations in e-voting have been detrimental. Similarly, in Canada, the lack of federal or provincial standards has left many municipalities to make decisions largely in isolation. In both cases, reliance on vendors to set the bar for cybersecurity and public accountability has been problematic. Switzerland, another federal country, may offer a good example in this respect: unlike other aspects of elections, internet voting is primarily and mainly regulated at the federal level, ensuring the same standards throughout the country. This is not (yet) the case with respect to other digital solutions used in elections, such as pure e-counting: cantons have so far resisted attempts to have federally harmonised/centralised regulations.

8. Content of regulation

a. Detailed requirements

Detailed regulation is important for commissioning digital solutions for elections, for control and certification procedures, for clarifying stakeholders' rights and obligations, and for informing digital solutions innovators and providers on the requirements.

The Venice Commission or OSCE/ODIHR have stressed that provisions for the use of technology need to be accompanied by detailed elaborations in the law on the technical solutions used and the procedures to be followed. These should cover, amongst others, aspects related to procurement, testing, auditing, and public access to the technologies. They emphasise that stating general principles is not enough when regulating digital solutions for elections if there is no guarantee that these general principles will be implemented with specific rules that are fundamental to genuinely democratic elections. It is thus necessary that regulations are drafted in a detailed and accountable manner.

When introducing new technologies in some parts of the electoral cycle, namely in voting and counting, a conflict arises between the requirements of secret suffrage and accuracy. For instance, the voter should be able to verify that his/her vote was registered and counted according to his/her will (accuracy) but at the same time he/she should not receive proof that enables him/her to sell his/her vote or to prove to a coercer how he/she voted (secrecy). The public should be able to verify the correctness of the result (accuracy), without learning how individual voters voted (secrecy). Cryptography provides solutions that accommodate such conflicting requirements up to a certain extent. It is not possible however to satisfy completely and simultaneously all conflicting requirements. Cryptographic solutions are based on assumptions that some participants in the process are honest for example. Such assumptions directly influence the implementation of the higher-level general principles and should be regulated in detail, by the competent authority.

b. Human-rights centred

It is now globally admitted that ICT participation tools should be human-rights compliant by design. This points to the necessity, in our case, of having detailed regulation that clarifies the implications of human rights (in this case the right to free, fair, and democratic elections) on the use of digital solutions in elections. Such regulation should precede the development and introduction of a specific solution. Solution developers should orient their work so that they take account of the regulatory requirements. They should know beforehand the main implications of free, fair, and democratic election principles on the considered technology.

Again, this shows that the legislator should be proactive and consider the broad use of digital solutions in the electoral cycle. Below are a few elements (the list is far from exhaustive) of such a regulation.

c. Usability

Usability is an important aspect, and not only to obtain user-friendly solutions. It is important from a security perspective, too. To deploy their effect and minimise misuse/abuse, digital solutions should be understood and used properly. Users should be prepared to notice and handle any potential errors that may occur. It is important that such issues are addressed in the regulation so that users' competences and obligations are clarified. This also points to the importance of the education of expected users and other stakeholders, and necessary regulatory provisions on information and education.

d. Data protection

Data protection instruments should be considered when regulating e-voting. But, as mentioned above, electoral data are sensitive data and, as such, subject to stricter requirements which should be provided for in the electoral legislation.

It is to be noted that data protection in the case of elections means the protection of certain data from the data controller (for instance, the electoral authority). Vote secrecy requires that neither electoral authority nor other actors know how a voter has voted. The same authority should, at the same time, control access to the solution as such access is limited to the right holders only. This makes use of digital solutions for some aspects of elections, such as voting, particularly delicate.

The legislator is asked to make important decisions in this respect. For instance, it will be asked to weigh-up values like security and transparency or the freedom to vote. These decisions are the preconditions for the implementation of digital techniques.

Existing regulations, mainly for e-voting, have evolved and still need to do so. Appropriate control of data protection implementations is important. In view of the 2019 European Parliament election, the European Commission prepared a guidance document on the application of European Union data protection law in the electoral context.

e. Transparency

Transparency's role is to guarantee that the overall system and the specific, digital solution are functioning properly. That said, the regulator should define which parts of the system should be transparent; what the concrete implications are; who participates in the transparency exercise; how to ensure the required transparency and control it; how to sanction non-compliance; and how to deal with information that is revealed through transparency, etc. Furthermore, participants should be informed and should be capable of participating in the exercise, especially if transparency is part of the system's security.

Transparency also has another dimension: digital solutions are in some cases expected to make politics more transparent, fight corruption, improve public

services, meaningfully involve citizens in local policy making, etc. If properly regulated and implemented, they may even succeed in doing so.

Regulation of the transparency of digital solutions has considerably evolved in recent years going from security by obscurity approaches and black-box systems, to partial transparency (involvement of political parties and accredited observers in transparency exercises), to a more open approach involving the publication of source codes and other relevant documents, control by independent specialists, and ethical hacking of solutions, etc. Such transparency is considered part of the security measures.

f. Cybersecurity

Cybersecurity in elections has been an extremely topical issue in recent years. Countries have become aware that the use of digital solutions, especially internet connected ones, might enable a single actor (including a foreign power) to control elections; absent durable, tamper-evident proof of the correct result/data. Regulatory frameworks should address risk strategies, protection measures, verification possibilities, and contingency planning, amongst others.

With respect to risk strategies, protection measures and contingency planning, guidance exists at the regional level, based on international legal instruments that address cybersecurity. The Committee of the Council of Europe Budapest Convention on Cybercrime has, for instance, issued a Guidance Note on elections. The note addresses the use of the Budapest Convention's procedural powers and mutual legal assistance provisions in a specific criminal investigation or proceeding in election interference. The Budapest Convention criminalises several types of conduct (illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery). If done without having the right by individuals as well as companies or other groups, in the context of elections, such conduct violates free, fair, and democratic elections. With election interference often having an international dimension, the Budapest Convention offers guidance on international co-operation to counter such offences. Also, at the EU level, the NIS Co-operation Group has issued specific guidance focusing on the cybersecurity of technology used in elections. Its 2018 Compendium on Cyber Security of Election Technology is meant to share experiences and provide guidance as well as an overview of tools, techniques and protocols to detect, prevent, and mitigate such threats.

With respect to verification options, the bulk of the effort is made in the e-voting field. Recent experiences show that the control of the set-up and implementation of verifiability solutions is crucial if they are to fulfil their role. However, the use of such methods is still in its infancy; their understanding by non-specialists is quite limited. More interdisciplinary understanding is required if such methods are to be imposed to ensure the security of the digital solutions used in elections.

g. Control, enforcement, accountability

The e-voting experience shows that regulation should include minimum requirements including for controlling the solution and for independently verifying both the solution and the results delivered by it (see the Recommendation CM/Rec(2017)5 on standards for e-voting).

Such requirements may apply beyond e-voting. They should fully reflect the free and fair democratic election principles and other relevant legal principles. Digital solutions should be subject to evaluations by independent and competent bodies, at appropriate intervals and after important changes. They should be open to audits and actively report on potential issues and threats.

Ultimate responsibility for the respect of requirements, even in the event of failures and attacks, lies with the authority responsible for conducting the task entrusted to the digital solution. The authority must conduct controls to satisfy itself that the solution and all related material and procedures are genuine, operate correctly, are kept up to date, are protected, and are operated in a secure manner. The solution should reflect the state-of-the-art, which means that co-operation with academia (independent and competent experts) is important. Experience with e-voting shows that it is challenging and it may be difficult to maintain state-of-the-art solutions over time.

As mentioned above, for critical and internet exposed solutions, controls (certification, audits, etc.) may not be enough. Independent verification of the results is needed. Verification may take different forms depending on the solution. It may itself be digital, or paper-based, or a combination of the two. For digital verification tools, experience shows that control of the controllers, namely control of the verification system, is necessary. Additionally, to correctly play their role, verifiability solutions need to be understood and employed by the users, which may be voters, election administration, observers, etc. It is therefore necessary to have knowledgeable users that make correct use of the solution. Certain attacks, for instance, can only be detected if enough end-users conduct the verification, understand the problem revealed by the verification, and complain.

More than ten years ago, the German Constitutional Court stated that certification is not enough and verification by the voter is needed. The Court did not accept the argument that it could be expected that the systems deployed were viable given that they had been examined and certified in a designated procedure prior to their deployment. The Recommendation of the Committee of Ministers of the Council of Europe CM/Rec(2017)5 on standards for e-voting prescribes individual and universal verification of the vote and of the overall results (see, in particular, standards 15 to 18) – two crucial outcomes of e-voting systems. This helps to ensure free suffrage.

The German or Austrian verification model requires that verification is understood and conducted by the layperson (the voter or the electoral commissioner) without any technical knowledge. This requires the co-existence, in parallel to the digital solution, of a paper-based one that can be understood by the layman. The other

verification model is the Estonian or Swiss one. The verification method can be controlled and validated by experts, who refer to methods approved by the respective scientific community. However, it seems difficult to apply such methods to political elections on a one-for-one basis.

h. Change management, resources, and cooperation with the private sector

Another difference between traditional and digital solutions is the evolving character of the digital technique. Regulation should integrate and reflect this. Closely linked to the evolving nature of technology, is the fact that digital solutions require qualified human resources and financial ones. Over time, the need for resources may fluctuate depending on the efforts necessary to ensure constitutional compliance of the solution. The need for resources and the prospect that such need may evolve in time should be properly addressed in the regulation. EMBs that have introduced digital solutions face the challenge of maintaining and replacing software and hardware. There are concerns about the sustainability of some electoral technology. It may be wise to consider such issues in the regulatory phase and perhaps avoid the most complex technologies.

An important aspect is the necessary co-operation with the private sector. The private sector may play several roles, including solution provider, controller, certifier, operator, etc. Given this fact, the legislator should carefully consider the relationship between the public and private sector. Detailed requirements that ensure respect for the higher-level principles should be foreseen in the procurement documents already. Ultimate responsibility for the conduct of the election lies with the state authority in charge of conducting the election. The regulation should address accountability and control requirements and, as experience shows, regulate the consequences of possible deficiencies. The legislator should carefully consider and ideally avoid dependence on private providers for sensitive solutions that critically impact the whole election. In addition, the authority should have enough qualified staff and should invest in its training to guarantee system maintenance, to facilitate the introduction of new features and other modifications, and to enable its proper functioning.

9. Trust

Trust is often mentioned when discussing the use of digital solutions in elections. It has different facets.

Trust is considered as a precondition to introducing digital solutions in elections. This is clear for electronic voting, but also applies to other digital solutions; for instance, to biometric technology. The introduction of technology cannot resolve a lack of trust in the electoral system. There have been other approaches in the past. Some of the earliest and keenest adopters of digital technologies for elections have been from amongst the poorest countries, often without a long history of democratic elections. In these contexts, adopting new and sometimes costly technology was designed to fight abuses and create trust between electoral

stakeholders and in the electorate. Initially, some countries succeeded in doing so. However, it has become clear that digital solutions alone cannot create trust. Existing trust, especially in the authorities in charge of conducting elections, is a precondition to the introduction of digital solutions. Where the public or political stakeholders mistrust each other or the digital solutions, these are not accepted, despite the objective technical merits and advantages that they might have. Existing trust as well as public consultation and backing are needed for a successful introduction of digital solutions. Experience shows that consultations, testing, piloting, etc. may help to instil confidence. However, the solution should be trustworthy first.

Research has attached a lot of importance to the trustworthiness of digital technologies in elections. This relates to state-of-the-art requirements, controls, implementations, solutions validated by peers, etc. However, in many cases, technology has been introduced without adequate research, planning, testing, training or voter education, and this has instead eroded trust in the process and increased costs. Elsewhere, technologies have been introduced that are not trustworthy and threaten electoral integrity, and this may lead to an erosion of public confidence in electoral processes.

Trust is based on transparency. It is not enough that solutions are trustworthy, and an election is free, fair, and democratic – the people must also be confident that this has been the case, according to Germany's Constitutional Court. Compliance with the constitutional principles of free, fair, and secret suffrage, etc. means that elections should be accompanied by people's confidence in compliance. For the German Constitutional Court, the only way to achieve this is to allow everyone to verify compliance.

CONCLUSIONS

Below, we summarise the main findings.

1. Digital solutions are already used in the electoral cycle. They must comply with all relevant **constitutional principles**, more specifically, with the principles of free, fair, and democratic elections.

   - Unlike the regulation of low-tech solutions, it is not enough for regulations of digital solutions to just restate the principles. They should include detailed provisions which translate the principles into detailed legal requirements that govern digital technology.

   - The challenge for the legislator is to ensure, already at the regulatory level, that constitutional rights are respected.

2. **International instruments** that regulate elections are relevant when envisaging the regulation of digital solutions used in elections. They include universal conventions (Universal Declaration of Human Rights, International Covenant on Civil and Political Rights) and regional ones (European Convention on Human Rights, EU Charter of Fundamental Rights), authoritative interpretations of such conventions, case law from international courts, political commitments, soft-law documents, studies and evaluations of existing regulations, and the uses of the digital solutions.

3. **International instruments** that regulate data protection, cybercrime or cybersecurity are also relevant.

   - Council of Europe Modernised Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108+) and the EU General Data Protection Regulation (GDPR) are highly relevant, however, some election data are qualified data: they require stricter protection which should be defined in election-specific regulations.

   - In the framework of the EU General Data Protection Regulation (GDPR), the Council of Europe Budapest Convention on Cybercrime and the EU legal instruments on cybersecurity, specific guidance and collections of good practices targeting elections have been developed.

4. **National regulations for digital solutions** used in elections are still in their infancy and evolving.

   - Specific regulations concern mainly e-voting. There have principally been two kinds of regulation. In some countries, older instruments that regulated the use of low-tech solutions evolved to govern e-voting machines. However, most of them were found to be constitutionally non-compliant, which led to the suppression or drastic reduction of the use of e-voting machines. First-generation internet voting regulations have also been judged insufficient. In some places, they were updated to reflect

a better understanding of digital technologies (risk policy, verifiability, independent controls, transparency requirements). However, recent experience shows that they need to continue to evolve to better address issues such as verifiability or transparency.

- Other digital solutions are under-regulated.

5 Clearly **identifying the problem** that needs to be solved is the first step towards finding an appropriate solution.

- Proposals for digital solutions should draw on research about the problem and users' expectations.
- Such assessments should be widely shared.

6 The next step is to identify the desired situation (the **goal**) and set **objectives** towards that goal.

- Goals and objectives should be "solution neutral".
- After identifying them, the legislator should consider all possible solutions with the aim of finding those that better contribute towards strengthening the constitutional principles.

7 To assess the option of introducing an envisaged solution, the legislator should consider both its **benefits and downsides**.

- The legislator should have a good understanding of benefits, downsides and respective solutions to be able to make meaningful assessments and make good decisions.
- As a rule of thumb, to counter shortcomings, it is important to be patient with the introduction of digital solutions. Clear objectives, feasibility studies, and pilots should precede and guide the introduction of digital solutions in the electoral process.
- We suggest that the periodic evaluation of benefits and downsides after the solution should be introduced and that periodic reassessment of such solutions is necessary.

8 The legislator should think as broadly as possible, in terms of the use of digital solutions throughout the **electoral cycle**.

- Solutions may evolve rapidly whereas the main features of the underlying technique will very likely persist over the long run. We suggest that such features must be regulated for the whole cycle. The ambition should be to understand and regulate the use of digital technology throughout the cycle, not just for specific solutions.
- The degree of automation of the electoral cycle, the lifespan of the different technologies used and the critical review of processes whose digitisation is being considered are important.

9 Regulation of digital solutions requires a **multidisciplinary approach**.

- As an initial step, several glossaries have been developed in recent years that explain legal and technical terms for the attention of specialists in both fields. This is necessary and important but not sufficient.
- As digital solutions are based on mathematics, programmers employ formal/rigid definitions of the relevant legal concepts to build digital solutions. In practice, however, legal principles are defined broadly and interpretation is necessary. There is no such strict definition of a legal concept. With respect to digital solutions, it is important that interpretations of principles for the respective technology are eventually decided by the competent authority (legislator or regulator) and are not left to solution providers or technicians alone.
- We suggest that multidisciplinary work requires iterative exchanges between legal and technical experts. The legislator must foresee adequate frameworks, resources and time for this important dialogue to take place and this should become the norm when regulating digital solutions for elections.

10 No international guiding document requires countries, respectively legislators, to introduce digital technologies in elections. This is **a sovereign decision**. Each society, namely legislator, has to decide if it is ready and able to introduce such modernisation. A good approach is to conduct tests that will provide important information for decision taking.

11 **Necessity**, **form,** and **level of regulation**

- The regulation is the founding layer of a constitutionally compliant digital solution. It is expected to offer guidance on the development of solutions. The legislator should proactively regulate the main aspects of the use of digital technologies in elections, in a solution-neutral way.
- Regulation cannot just restate principles or proceed by analogy with paper-based solutions. It should clearly indicate the practical implications of the principles and enable independent controls to make sure that detailed requirements are respected.
- Definition of the concrete meaning of higher principles in a context where digital solutions are used affects the very meaning of the principles. So, the decision eventually has to be taken by the competent authority, usually the legislator.
- Delegation of regulatory powers to the government, or the central election commission etc., should be clearly framed.
- Regulatory aspects are more complex in federal states with a decentralised system of administering elections. It is important to make sure that the same legal standards apply throughout the country and in the solutions.

12 **Detailed requirements** are important. Stating general principles is not enough when regulating digital solutions for elections if there is no guarantee that these general principles will be implemented with specific rules that are fundamental to genuinely democratic elections. It is therefore necessary that regulations are drafted in a detailed and accountable manner. Detailed requirements are particularly important when introducing cryptographic solutions.

13 Participation tools should be **human-rights compliant by design**. Solution developers should orient their work to take account of the detailed regulatory requirements for digital solutions. They should know in advance the main implications of free, fair, and democratic election principles on the technology under consideration.

14 **Usability** is important from a user-friendliness perspective and also as it contributes to the security of the digital solution.

15 Some electoral data are sensitive data.

- **Data protection** in this case means the protection of certain data from the data controller (for example, the electoral authority). The same authority should, at the same time, control access to the solution as such access is limited to right holders only. This makes use of digital solutions for some aspects of elections, such as voting, particularly delicate.
- The legislator will have to weigh-up opposing values like security and transparency or freedom to vote. Such decisions are preconditions to the implementation of digital technique.

16 Regulation of the **transparency** of digital solutions has evolved towards a more open approach.

- This involves publication of source codes and other relevant documents, control by independent specialists, ethical hacking of solutions, etc. Such transparency is considered part of the security measures.
- The regulator should define which parts of the system should be transparent, what the concrete implications are, who participates in the transparency exercise, how to ensure the required transparency and control it, how to sanction non-compliance, how to deal with information that is revealed through transparency, etc.

17 **Cybersecurity** for elections has been an extremely topical issue in recent years. Regulatory frameworks should address risk strategies, protection measures, verification possibilities, and contingency planning, amongst others.

- With respect to risk strategies, protection measures and contingency planning, guidance exists at the regional level, based on international legal instruments that address cybersecurity.

- With respect to verification possibilities, the bulk of efforts are made in the e-voting field. Control of the set-up and implementation of verifiability solutions is crucial if they are to fulfil their role. More interdisciplinary understanding is required if such methods are to be imposed to ensure the security of the digital solutions used in elections.

18 Control, enforcement, accountability

- Regulation should include minimum requirements for controlling the solution and for independently verifying both the solution and the results delivered by it.
- Ultimate responsibility for the respect of requirements even in the case of failures and attacks lies with the authority responsible for conducting the task entrusted to the digital solution.
- The solution should reflect the state-of-the-art, which means that co-operation with academia (independent and competent experts) is important. This may be challenging to ensure over time.
- For critical and internet exposed digital solutions, controls (certification, audits, etc.) may not be enough. Independent verification of the results is needed. Verification may take different forms.
- For digital verification tools, experience shows that the control of controllers, namely control of the verification system is necessary.
- Verifiability solutions need to be understood and actually used by end-users, which may be voters, election administration, observers, etc. Certain attacks, for instance, can only be detected if enough end-users conduct the verification, understand the problem revealed by the verification and then complain.

19 Change management

- The evolving character of the digital technique should be integrated in its regulation.
- Closely linked to the evolving nature of technology, is the fact that digital solutions require qualified human resources and financial ones. The need for resources and the prospect that such need may evolve in time should be properly addressed in the regulation.
- The legislator should carefully consider the relationship between the public and private sector. Detailed requirements that ensure respect for the higher-level principles should be foreseen in the procurement documents in advance.
- Ultimate responsibility for the conduct of the election lies with the state authority in charge of conducting the election. The regulation should

address accountability and control requirements and, as experience shows, regulate the consequences of possible deficiencies.

- The authority should have enough qualified staff and should invest in its training.

20 Trust

- Trust is considered as a precondition to introducing digital solutions in elections.
- Solutions should first be trustworthy. This relates to state-of-the-art requirements, controls, implementations, solutions validated by peers, etc.
- Trust is based on transparency and verification possibilities.

SELECTED REFERENCES

International legal texts, guidance, evaluations, good practice

Council of Europe, *Convention for the Protection of Human Rights and Fundamental Freedoms, (European Convention on Human Rights, ECHR) (in force, 1953).*

Council of Europe, *Modernised Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108+), CETS № 223 (Protocol adopted in June 2018).*

Council of Europe, Consultative Committee of Convention 108+, *Report on Artificial Intelligence. Artificial intelligence and data protection: challenges and possible remedies (January 2019).*

Council of Europe, *Convention on Cybercrime (Budapest Convention), CETS № 185 (in force, 2004).*

Council of Europe, Cybercrime Convention Committee (T-CY), *Guidance note № 9, Aspects of election interference by means of computer systems covered by the Budapest Convention. Adopted by T-CY on 8 July 2019.*

Council of Europe, European Court of Human Rights, *Guide on Article 3 of Protocol № 1 to the European Convention on Human Rights - Right to free elections (April 2019).*

Council of Europe, Committee of Ministers, *Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting (Adopted by the Committee of Ministers on 14 June 2017 at the 1289th meeting of the Ministers' Deputies).*

European Union, *Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).*

European Union, *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, (NIS Directive).*

European Union, NIS Co-operation Group, *Compendium on Cyber Security of Election Technology, CG Publication 03/2018.*

European Union, *Regulation (EU) 2016/679 General Data Protection Regulation, (GDPR).*

European Commission, *Free and Fair Elections. Guidance Document. Commission guidance on the application of Union data protection law in the electoral context (September 2018).*

European Union (Council of the), *Council Directive 94/80/EC of 19 December 1994 laying down detailed arrangements for the exercise of the right to vote and to stand as*

a candidate in municipal elections by citizens of the Union residing in a Member State of which they are not nationals.

European Union, *Act concerning the election of the representatives of the Assembly by direct universal suffrage, OJ L 278, 8.10.1976, p. 5 as amended lastly by Council Decision 2002/772/EC, Euratom of 25 June and 23 September 2002.*

European Union (Council of the), *Council Decision 2018/994* [not in force] *amending the Act concerning the election of the members of the European Parliament by direct universal suffrage, annexed to Council Decision 76/787/ECSC, EEC, Euratom of 20 September 1976.*

European Union, Estonian Presidency of the Council of the EU, *Tallinn Declaration on eGovernment (Oct. 2017).*

European Union, *Regulation No 211/2011 of the European Parliament and of the Council of 16 February 2011 on the citizens' initiative.*

European Commission for Democracy through Law (Venice Commission) et al., *Joint Report on Digital Technologies and Elections (June 2019).*

European Commission for Democracy through Law (Venice Commission), *Compilation of Venice Commission opinions and reports concerning digital technologies in the electoral process, CDL-PI(2018)011 (2018).*

European Commission for Democracy through Law (Venice Commission), Grabenwarter, Ch. *Report on the compatibility of remote voting and electronic voting with the standards of the Council of Europe, 2004.*

European Commission for Democracy through Law (Venice Commission), *Code of Good Practice on Electoral Matters - Guidelines and explanatory report* (2002).

IDEA*, Cybersecurity in Elections. Models of Interagency Collaboration, 2019.*

IDEA, RECEF, *The Use of New Technologies in Electoral Processes - Workshop report: Praia, Cabo Verde, 22–23 November 2017.*

IDEA, *Certification of ICTs in Elections, 2015.*

IDEA, *Electoral Management Design, Revised Edition, 2014.*

IDEA*, International Obligations for Elections, Guidelines for Legal Frameworks, 2014.*

IFES, Goldsmith, B./Ruthrauff, H., *Implementing and overseeing Electronic Voting & Counting Technologies, 2013.*

OSCE/ODIHR, *Handbook for the observation of new voting technologies, 2013.*

OSCE/ODIHR, *Guidelines for reviewing a legal framework for elections, 2013.*

OSCE/ODIHR, See "Needs Assessment Mission" and "Election Assessment Mission" Reports on elections held in countries of the Council of Europe region. See in particular "Legal Framework", "New Voting Technologies" and "Recommendations" sections of the respective reports, available at www.osce.org/elections.

UN Secretary General's High-level panel, *The age of digital interdependence, June 2019.*

UN General Assembly, Human Rights Council, Report of the Office of the United Nations High Commissioner for Human Rights – Draft guidelines for States on the effective implementation of the right to participate in public affairs (September 2018).

Relevant research on legal and regulatory aspects

Barrat J. *(2016),* (Coord.) *El voto electronic y sus dimensiones jurídicas: entre la ingenua complacencia y el rechazo precipitado, Iustel.*

Barrat J. and Goldsmith B. *(2012), Compliance with International Standards, Norwegian e-vote project.*

Benaloh J., Rivest R., Ryan P. et al. *(2014), End-to-end verifiability.*

Cardillo et al., *Online Voting in Ontario Municipal Elections: A Conflict of Legal Principles and Technology?, in Krimmer R. et al. (Eds.), E-Vote-ID 2019.*

Driza Maurer A., *The Swiss Post/Scytl Transparency Exercise and its possible Impact on Internet Voting Regulation, in Krimmer R. et al. (Eds.): E-Vote-ID 2019.*

Driza Maurer A., Barrat J. (Eds), *E-Voting Case Law: A Comparative Analysis, Routledge 2017.* The publication includes chapters on the legal framework of digital technologies used in elections in Germany, Austria, Brazil, India, Estonia, France, Argentina, Finland, Mexico, Switzerland, USA, Australia and Venezuela.

Driza Maurer A., *Updated European Standards for E-voting. The Council of Europe Recommendation Rec(2017)5 on Standards for E-voting, in R. Krimmer et al. (Eds.): E-Vote-ID 2017.*

Driza Maurer A. *(2016), Update of the Council of Europe Recommendation on Legal, Operational and Technical Standards for E-Voting – a Legal Perspective. In: Tagungsband IRIS (Internationales Rechtsinformatik Symposion).*

Driza Maurer A., *Ten Years Council of Europe Rec(2004)11. Lessons learned and outlook. In: Krimmer, R., Volkamer, M. (eds) (2016), Proceedings of Electronic Voting 2014.*

Driza Maurer A., *Internet Voting and Federalism: The Swiss Case, In Barrat J. (Coord.) El voto electronic y sus dimensiones jurídicas : entre la ingenua complacencia y el rechazo precipitado, Iustel.*

Gibson P., Krimmer R. et al (2016), *A review of E-voting: the past, present and future.*

Hill R., *E-Voting and the Law. Issues, Solutions, and a Challenging Question. In Krimmer, R. et al. (eds.), Proceedings of E-VOTE-ID 2016.*

Krimmer et al. (Eds), See proceedings of E-Vote-ID Conferences, 2019, 2018, 2017, 2016.

Loeber L., *Legislating for e-enabled elections: dilemmas and concerns for the legislator. In Krimmer R. et al. (eds.) Proceedings of E-VOTE-ID 2016.*

Loeber L. *"E-Voting in the Netherlands; from General Acceptance to General Doubt in Two Years" in Krimmer, R. and Grimm R. (Eds) (2008), Electronic Voting 2008 (EVOTE08).*

Madise Ü. and Vinkel P. (2011), *"Constitutionality of Remote Internet Voting: The Estonian Perspective", Juridica International.*

Mohanty et al. (2019), *Auditing Indian Elections.*

Neumann S., Volkamer M., *A Holistic Framework for the Evaluation of Internet Voting Systems. In: Zissis D., Lekkas D. (eds) (2014), Design, Development and Use of Secure Electronic voting Systems, IGI Global book series*

Neumann S. (2016), *Evaluation and Improvement of Internet Voting Schemes Based on Legally-Founded Security Requirements.*

Puiggali J., Rodriguez-Peréz A., *Designing a national framework for online voting and meeting its requirements: the Swiss experience. In Krimmer et al. (eds) E-Vote-ID 2018 Proceedings.*

Saltman Roy (2008), *The History and Politics of Voting Technology. In Quest of Integrity and Public Confidence.*

Schwartz B. and Grice D. *(2013), Establishing a legal framework for e-voting in Canada.*

Solvak M., Vassil K., *E-voting in Estonia: Technological diffusion and other developments over ten years (2005-2015).*

Spycher O., Volkamer M. and Koenig R. *(2011), Transparency and technical measures to establish trust in Norwegian internet voting.*

Taylor G. *(2010), Constitutional restrictions on touch-screen voting computers in Germany, in Election Law Journal, Volume 9, Number 4.*

Venice Commission/Permanent Electoral Authority of Romania, *Electoral Expert, Proceedings of the 1st Scientific Electoral Experts Debates "Electoral Law and New Technologies: Legal Challenges", Bucharest, 12 - 13 April 2016* (several experts' contributions).

Vinkel P. (*2015*), *Remote Electronic Voting in Estonia: Legality, Impact and Confidence, TUT Press.*

Volkamer M., Spycher O. and Dubuis *E. (2011), Measures to establish trust in internet voting.*

Volkamer M. (2009), Evaluation of Electronic Voting, Requirements and Evaluation Procedures to Support Responsible Election Authorities, Springer-Verlag Berlin Heidelberg.

Relevant documents from selected countries

Austria, *Students' Union Act (Bundesgesetz über die Vertretung der Studierenden [Hochschülerinnen- und Hochschülerschaftsgesetz 1998 – HSG 1998]), Federal Law Gazette I 1999/22, last amendment Federal Law Gazette I 2013/79. In 2014, the Students' Union Act 1998 was substituted by the Students' Union Act 2014, Federal Law Gazette I 45/2014.*

Austria, Constitutional Court *(Verfassungsgerichtshof) Decision V 85-96/11-15, 13 December 2011. For a detailed discussion, see the chapter on Austria by Melina Oswald, "E-Voting in Austria: Legal Determination Matters" in Driza Maurer/Barrat (Eds), E-Voting Case Law: A Comparative Analysis, 2017.*

Belgium, (Law on e-voting with paper audit trail) *Loi du 7 fevrier 2014 organisant le vote électronique avec preuve papier (Moniteur belge du 14 février 2014).*

Finland, Ministry of Justice, *Working Group Report "Online voting in Finland – Feasibility study" 19.12.2017.*

France, Commission Nationale de l'Informatique et des Libertés (CNIL), *Délibération n° 2019-053 du 25 avril 2019 portant adoption d'une recommandation relative à la sécurité des systèmes de vote par correspondance électronique, notamment via Internet.*

France, *Rapport d'information n° 73 (2018-2019) de Mme Jacky Deromedi et M. Yves Détraigne, fait au nom de la commission des lois, déposé le 24 octobre 2018 "Réconcilier le vote et les nouvelles technologies".*

France, Sénat, Commission des lois, *Rapport d'information de MM. Alain Anziani et Antoine Lefevre, "Vote électronique: Préserver la confiance des électeurs" 2014.*

Germany, *Ordinance on the Use of Vote Counting Devices in Elections to the German Bundestag (Verordnung über die Verwendung von Stimmenzählgeräten bei Wahlen zum Deutschen Bundestag) (BGBl. 1961 I 1618).*

Germany, Constitutional Court *(Bundesverfassungsgericht), Decision 2 BvC 3/07, 2 BvC 4/07, of 3 March 2009. For a detailed discussion, see the chapter on Germany by Sebastian Seedorf, "Germany: The Public Nature of Elections and its Consequences for E-Voting" in Driza Maurer/Barrat (Eds), E-Voting Case Law: A Comparative Analysis, 2017.*

Netherlands (The), Election Process Advisory Commission, *Report: Voting with confidence. Summary, Conclusions and Recommendations (2007).*

Swiss *Federal Chancellery Ordinance on Electronic Voting (VEleS), RS 161.116.*

Swiss *Federal Council,* (First Govt. report on the feasibility of e-voting) *"Rapport sur le vote électronique. Chances, risques et faisabilité" of 9 January 2002, FF 2002 612 (2002).*

Swiss *Federal Council,* (Second Govt. report on the evaluation of pilots) *"Rapport sur les projets pilotes en matière de vote électronique" of 31 May 2006, FF 2006 5205 (2006).*

Swiss *Federal Council,* (Third Govt. report on evaluation of expériences and basis for future development of e-voting) *"Rapport du Conseil fédéral sur le vote électronique. Evaluation de la mise en place du vote électronique (2006–2012) et bases de développement" of 14 June 2013, FF 2013 4519 (2013).*

Overview of digital technologies used in the electoral cycle**

Content

** This is an abridged version of the paper "New technologies in the electoral cycle. Guidance from the Council of Europe" presented by the author to the working group on democracy and technology of the European Committee on Democracy and Governance (CDDG) of the Council of Europe, on 28 January 2020. The European Committee on Democracy and Governance (CDDG) has been given the specific task of developing standards on the use of new technologies in the different stages of the electoral process. This task has been assigned by the working group on democracy and technology.

1. APPROACH AND DEFINITIONS

a. Introduction

The present paper gives an overview of the main digital technologies used or envisaged during an electoral cycle and identifies questions of conformity with the principles of democratic elections. This is an abridged version of the paper "New technologies in the electoral cycle. Guidance from the Council of Europe" presented at the working group on democracy and technology of the European Committee on Democracy and Governance (CDDG) of the Council of Europe, on 28 January 2020.[1]

As the guardian of the values enshrined in the European Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights or Convention) and its protocols, the Council of Europe has the core mission of overseeing the implementation of the Convention in the countries of the region, including in election-related activities. Pursuant to Article 3 of Protocol № 1 to the Convention and case law of the European Court of Human Rights, the Election Management Body (namely the State) has the positive obligation to ensure that all activities led by it within an electoral cycle comply with the right to free elections, including those backed by new technologies. This report focuses on the respect and implementation of Article 3 of Protocol № 1 to the Convention[2] by new technologies used in the electoral cycle. More specifically, the focus is on the principles of universal, equal, free and secret suffrage and on some conditions for implementing these principles (for example, procedural guarantees of impartiality, transparency and observation, etc.).[3] Other election-relevant principles, such as freedom of opinion and expression, freedom of peaceful assembly, freedom of association, freedom of movement, freedom from discrimination, the right to an effective legal remedy need to be considered too. However, they will not be discussed here.

Digital solutions improve and facilitate electoral processes, but they also bring challenges and risks. They may increase efficiency and speed, help to avoid the errors of manual work, etc., but they may also create new vulnerabilities, expose the electoral system to new threats and enable new attacks on it. The regulator must take informed decisions so that new technologies are introduced and operated

1. To learn about the work of the Council of Europe in elections and get guidance on the use of digital technologies in the electoral field, consult www.coe.int, in particular, the current work of the European Committee on Democracy and Governance (CDDG), that of the Electoral Assistance Division and of the European Commission for Democracy through law (Venice Commission), amongst others.

2. 45 out of 47 member states have ratified this protocol. Switzerland and Monaco have signed it but not yet ratified it. However, with the exception of the accepted lack of secrecy in (only) some local elections where voting by raising hands is used, the electoral principles of Swiss law are usually considered to be stricter compared to P1-3 ECHR.

3. Venice Commission, Code of good practice in electoral matters, Opinion № 190/2002, adopted by the Venice Commission at its 52nd session (Venice, 18-19 October 2002); CDL-AD (2002) 23 rev. The application of the principles of direct suffrage and the frequency of elections does not seem to be affected by the technology used in the electoral cycle.

in a secure way. Secure use implies that digital solutions (as with any aspect of an election) comply with the principles of democratic elections and thus ensure universal, equal, free and secret suffrage, amongst others.

All countries in the region have subscribed to minimum international standards for democratic elections. These are found in Article 25 of the 1966 International Covenant on Civil and Political Rights (ICCPR) and Article 3 of Protocol № 1 to the European Convention on Human Rights[4] on the right to free elections.[5] They are further elaborated in political commitments (the 1990 CSCE Copenhagen Document commits participating States to guaranteeing human rights and fundamental freedoms, including those pertaining to elections), jurisprudence of the European Court of Human Rights and soft law (1996 UNHRC General Comment № 25 and the Venice Commission's 2002 Code of Good Practice in Electoral Matters and 2007 Code of Good Practice on Referendums).

The paper gives an overview of some new technologies that have been introduced or considered for use in the electoral cycle, their main features and conformity issues. Then, it looks at the different phases of the electoral cycle and to the digital solutions used or considered and their conformity. It ends with a summary and some transversal questions relevant to all new technologies and all phases of the electoral cycle.

The paper builds on previous work at the Council of Europe in the e-voting field (see Recommendation CM/Rec(2017)5 on standards for e-voting, hereinafter Recommendation CM/Rec(2017)5). Also, work by the Venice Commission, the Council of Europe Division on electoral assistance and civil society, the Council of Europe Convention on Cybercrime (Budapest Convention) and the Modernised Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108+), as well as work by other organisations such as the OSCE/ODIHR, International IDEA, the EU, etc. is considered.

b. Electoral cycle

An electoral cycle encompasses all steps and processes that are necessary for an election or vote to take place.[6] The Election Management Body (EMB), the authority in charge of organising elections, carries out and/or controls the activities of an electoral cycle. The notion of a "cycle" also implies that these steps are repeated at

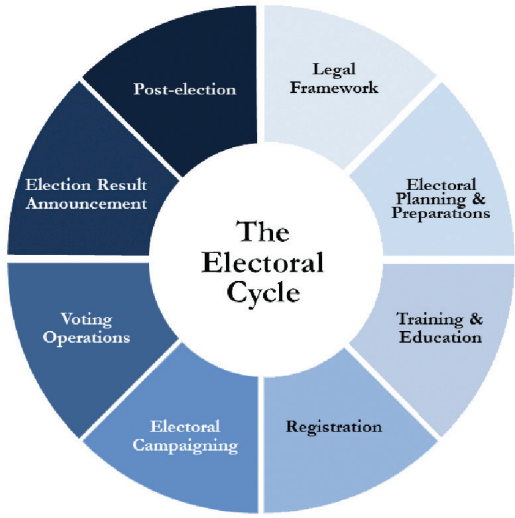
4. 45 of the Council of Europe's 47 member states have ratified this Protocol. Switzerland and Monaco have signed it but not yet ratified it. However, in Switzerland, for example, federal and cantonal electoral principles are de facto stricter compared to Article 3 of Protocol № 1 to the Convention. The only exception is the lack of secrecy in some local elections where voting by raising hands is used, which is accepted by the Supreme Court for historical and practical reasons, despite criticism by legal doctrine.

5. Article 3 of Protocol № 1 to the Convention states "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."

6. We refer to the election cycle as defined by IDEA in *Electoral Management Design, 2014: 12; 16; 75-77*, with minor changes and complements.

regular intervals, for each election.[7] The main phases of an election cycle are the following:

1. **Legal framework**. This includes the design and drafting of legislation.
2. **Planning and preparation** for the implementation of electoral activities. This includes the recruitment and training of electoral staff as well as electoral planning.
3. **Training and education** of voters, regulation of conduct of observers.
4. **Registration** of voters, political parties and election observers; nomination of parties and candidates. Registration and handling of issues/questions potentially leading to a referendum (popular vote).



Source: IDEA

5. **Electoral campaigning**, including official information addressed to electors.
6. **Voting operations**, including polling, counting and tabulating results.
7. **Election results** announcement, including transmission and publication of results, the resolution of electoral disputes, reporting, auditing.
8. **Post-election** duties including the destruction and/or archiving of materials.[8]

The conduct of direct democracy votes involves similar steps and additional ones, such as the formal and/or material approval of the proposal (initiative or referendum), control of the form for gathering signatures of supporters, reception and control of validity of signatures, counting, validation and publication of results and, eventually, the organisation of the vote if the required number of valid signatures was successfully collected. We include all these steps in the registration

7. The electoral cycle was conceptualised by International IDEA and the European Commission in 2005. The purpose was to illustrate the fact that elections are not events but processes, and to mainstream this knowledge throughout the planning and implementation phases of all electoral assistance projects – aiming at longer-term commitments of funds and other resources, a focus on sustainability within electoral institutions and an overall commitment to the democratic development of a country far beyond the immediate event to be supported, https://www.idea.int/data-tools/tools/online-electoral-cycle

8. The actual chronological sequence of the phases may be different from the one presented above.

phase (№ 4 above). After that, the EMB informs voters, plans and conducts the vote, etc. In this paper, the term election/electoral cycle refers to both elections and direct democracy votes.

The paper considers the use of new technologies in the different phases of the electoral cycle, with the exception of opinion formation and election financing issues, which are dealt in other work streams at the Council of Europe level.

c. New technologies

In this paper, "new" and "digital" are used as synonyms. Digital technologies and solutions employed, tested or envisaged in the electoral cycle are the digitisation of documents and procedures, biometry, blockchain, cloud computing. Artificial intelligence is discussed, with the exception of its use in the opinion formation (electoral campaigning) field.

Digital solutions store and handle information digitally and cannot be observed or understood by the layperson. More complex technologies, such as artificial intelligence, may evolve so that their detailed functioning is not understood even by the engineers who built them. So, the principle feature of such technologies is their complexity. Furthermore, they evolve rapidly. This makes them qualitatively different from "old" paper-based or mechanical technologies and solutions.

2. QUESTIONING THE CONFORMITY OF NEW TECHNOLOGIES WITH ARTICLE 3 OF PROTOCOL № 1 TO THE EUROPEAN CONVENTION ON HUMAN RIGHTS

a. Technology perspective

Digitisation

The existence of digital technology and its application to nearly all aspects of life, including elections, is a fact that cannot be called into question.[9] Digitisation is the first layer, which allows for computer treatment of information. It is the conversion of text, pictures, and sound into a digital form that can be processed by a computer.

Digitised data include voter registers, registers of candidates, results entered in electronic format, etc. Digitised processes include e-registering, e-identification of voters, e-voting on voting machines in polling stations or over the internet, e-counting (that is software used to register and calculate results and maybe also allocate seats), software used for statistical purposes, e-transmission of preliminary and/or final results, for example, from polling stations to a central unit, etc. Digitisation of processes is more challenging when they transit over the internet, due to cybersecurity issues. Digitised data and processes may be grouped in election information and management systems.

In the following paragraphs, we include information from a questionnaire prepared and distributed by the CDDG and to which several countries replied by the end of 2019. The questionnaire was short and focused on the implementation of the Recommendation CM/Rec(2017)5. The answers were provided by different offices, not systematically by EMBs. Despite these limitations, the replies provide a current, although not exhaustive, overview of the digital technologies used in electoral processes.

E-voting is the most supervised use of new technologies in the electoral cycle as it covers the most sensitive process of an electoral cycle, namely the actual vote and the result of an election. It is also the most advanced example of the use of new technologies because usually it is not just the digitisation of the voting and counting processes, but it ideally implies that all involved documents and processes are digitised so that transactions can take place without media discontinuity.

According to the Recommendation CM/Rec(2017)5, e-voting comprises the e-casting of the vote and the e-counting of paper ballots. E-casting of the vote includes both voting on electronic voting machines (hereinafter EVM) in polling stations and voting via the Internet from an uncontrolled environment (hereinafter

9. European Commission for Democracy through Law (Venice Commission) et al., 2019, "Joint Report on Digital Technologies and Elections"

i-voting). E-casting implies e-counting. There is also the pure e-counting of paper ballots using optical scanners which digitise the paper ballot and then proceed to the counting.

E-voting is practiced in a few countries, as shown in the replies to the questionnaire, including *Belgium* (EVM for all kinds of elections and referenda); *Bulgaria* (EVM only for national and the EU elections as well as the election of the president and vice-president of the Republic of Bulgaria but not for referenda); *Estonia* (i-voting for all national elections but not for local referenda which make use of different technical solutions); the autonomous region of *Åland* in *Finland* (i-voting, recently suspended); *France* (EVM in 66 communes and i-voting for French expatriates during parliamentary and consular elections; at the local level, municipal councils may use i-voting to vote); *Iceland* and *Norway* (i-voting for local referenda only); *Russian Federation* (EVM for national and regional elections); *Switzerland* (i-voting for federal, cantonal and communal votes and elections; currently suspended).

The replies to the CDDG questionnaire show that pure e-counting (optical character recognition technology) is practiced in *Hungary* (for preliminary results only), *Latvia, Malta* (since May 2019 European Parliament and local council elections), *Norway*, *Switzerland* (some cantons scan and count paper ballots in referendum votes), the *Russian Federation* as well as the *United Kingdom* (*England* has used it since 2000 in local and national elections; *Scotland* used it in the 2007 local and national elections). On this occasion, significant errors were found in the ballot design. E-counting was used again in the 2012 and 2017 local elections, with success. The counting of the ballot papers [Single Transferable Vote system] has been reduced from three/four days to a matter of hours).

E-voting is envisaged in *Azerbaijan*, *France,*[10] *Romania*,[11] *Serbia*,[12] *Ukraine*,[13] the *United Kingdom*.[14] It has been partially or totally suspended or abolished in

10. A French Senate 2018 report (Deromedi, Detraigne) recommended using i-voting in consular elections in 2020 and in parliamentary elections in 2022. The French Government recently approved the i-voting solution for the 2020 election.

11. Romania's Permanent Electoral Authority is considering e-voting, however, according to the reply, implementation may not begin before the close of 2020 as some political actors and administrative institutions mistrust this technology.

12. A possible upcoming law on referenda and popular initiatives considers the e-initiative as an initial trial of e-voting in Serbia.

13. According to the reply, a law on national and local referenda that considers the e-voting option is being prepared.

14. A non-binding trial took place in May 2019 in a local election. It allegedly featured an end-to-end verifiable system comprising touch-screen computers at the polling booth, passcodes issued to electors, voter verifiable paper receipts, publication of encrypted votes on the election website, the system flagging up if any e-vote was illegitimately modified. The trial took place in a context where the Welsh and Scottish governments have proposed pilots of e-voting in local elections.

Bulgaria,[15] *Finland*,[16] *France*,[17] *Germany*,[18] *Ireland*, *the Netherlands*,[19] *Norway*,[20] *Switzerland* [21] and the *United Kingdom*.[22]

E-voting has been considered for political elections but not launched in *Austria*,[23] the *Czech Republic*, *Denmark*, *Finland*,[24] *Latvia*,[25] *Spain*.[26] The main arguments against the introduction of e-voting relate to security, complexity and cost.

The digitisation of documents and processes of the electoral cycle is however widespread. Here is an overview based on the answers to the CDDG questionnaire that were submitted at the end of 2019.

Basic data and processes are reportedly digitised in *Finland, Hungary, Latvia* (for example, electoral districts, municipalities, voting districts, election authorities, preparation and publication of candidate lists, preparation of ballot layouts).

Digitised services or processes that are used before voting day include e-services for electors to find or change their polling station (*Hungary*); to apply for postal voting (*Latvia*); or check and amend their electoral details (*Ireland*) or to register for voting abroad (*Spain*); signature collection for new parties wishing to stand for elections (*Denmark*); [27] signature collection for national or local referenda (*France*).

15. In 2019, the Bulgarian Parliament abolished e-voting for local elections due to the complexity of such elections and the financial cost of e-voting.

16. It was abolished after a 2008 municipal election test identified several problems.

17. Since 2008, a moratorium has suspended any extension of EVMs to new communes. At the last national elections, i-voting was cancelled. However, it is expected to be used in 2020 and 2022, as recommended by the Senate 2018 report.

18. Federal Constitutional Court decision of 3 March 2009, BVerfGE 123, 39. The decision declared the Federal Voting Machine Ordinance (*Bundeswahlgeräteverordnung of 3 September 1975, BGBl. 1975 I 2459, as last amended by Article 1 of the Ordinance of 20 April 1999, BGBl. 1999 I 749*) to be incompatible with the principle of the public nature of elections according to which the layman must be able to follow and understand the main steps in the election process without special technical knowledge.

19. In 2006, following decades of e-voting, the EVM came under heavy criticism in the Netherlands for the lack of security and auditability. Since 2008, voting is conducted using paper ballots only.

20. After holding trials in 2011 and 2013, in 10 and 12 municipalities respectively, Norway's government discontinued i-voting because of the lack of political will to establish it as a regular channel. It remains an option for local referenda only.

21. Swiss i-voting has, *de-facto*, been suspended since mid-2019 as no i-voting system fulfils the legal requirements.

22. After trials in local elections in England between 2002 and 2007, e-voting was discontinued mainly because of complexity and transparency issues; the risks were considered to outweigh the advantages and a clear vision, strategy, effective planning, cost-effectiveness, and system certification were lacking.

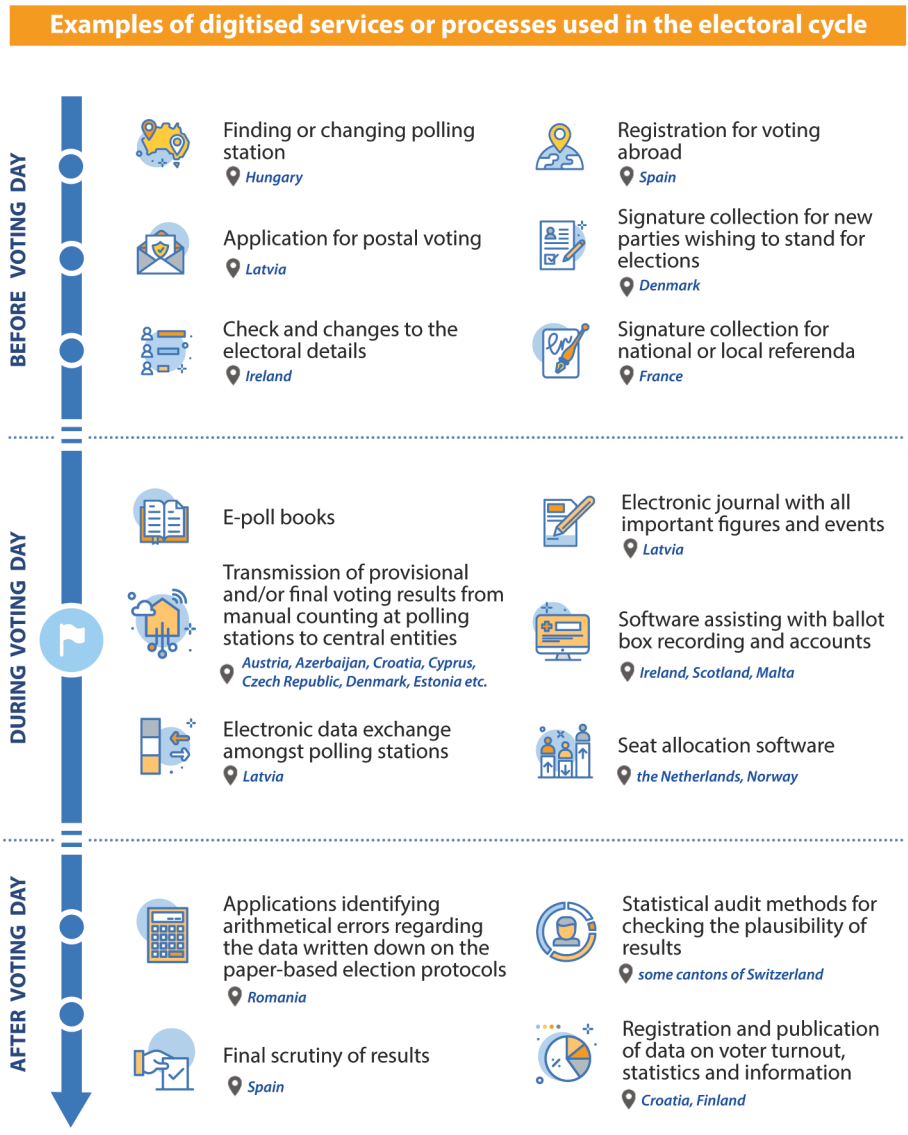
23. A Constitutional Court decision in 2011 established that the electoral commission must understand all steps and procedures of i-voting without assistance from technical experts, which is impossible to achieve.

24. A report concluded at the end of 2017 that i-voting risks currently outweigh benefits.

25. According to the reply to the questionnaire, some discussions in parliament show that the introduction of i-voting is again being reconsidered although it is not a popular concept.

26. I-voting has been discussed only for Spaniards living abroad.

27. After initial experiences and identified problems, the Danish Parliament decided in 2019 to procure a redesigned system.



Digitised services or processes available during and after voting day (outside of any e-voting) include the electronic *journal* with all important figures and events (*Latvia*);[28] e-poll books; electronic data exchange amongst polling stations, ensuring the opportunity for voters to vote at any polling station during early voting days (*Latvia*); transmission of provisional and/or final voting results from manual counting at polling stations to central entities where they are consolidated, counted and published, as the case may be (in *Austria, Azerbaijan, Croatia,*

28. A pilot project took place at the 2019 European Parliament Election in Latvia.

Cyprus, Czech Republic, Denmark, Estonia, Finland, Greece, Germany, Hungary, Latvia, Norway, Romania, Slovak Republic, Slovenia, Spain, the Netherlands); software assisting the returning officers with ballot box recording and accounts in accordance with the system of Proportional Representation-Single Transferable Vote (PR-STV) (*Ireland*, *Scotland, Malta*); seat allocation software (*the Netherlands*, *Norway,* etc.).

An important type of digitised document to be used almost everywhere in the region are registers: registers of voters and candidates, registers that keep track of those who have already voted during an election (use of voting rights). In addition to countries using *e-casting* for voting, they are also used in *Finland*, *Hungary*, *Latvia*, *Norway*, *Serbia*, and *Slovenia*.

Digitised services or processes available after voting day include solutions to *check* results, including applications identifying arithmetical errors regarding the data written down on the paper-based election protocols (*Romania*);[29] or statistical audit methods for checking the plausibility of results; final scrutiny of results (*Spain*);[30] registration and publication of data on voter turnout, statistics and information (for instance, in *Croatia* or *Finland,* amongst others).

Plans for the extension of the use of digital solutions in the electoral cycle are reported in several countries, namely *Denmark*, where an Election Management System is expected to be deployed in 2020; in *France* where e-signature gathering for referenda is envisaged; in *Finland*, where an Election Information System (EIS) is planned to be introduced; in *Ireland*, where electoral register modernisation is underway and a national roll out of online registration is being examined; in *Latvia*, where they intend to introduce an electronic voters' list for polling stations in the next municipal and parliamentary elections to deliver the possibility to vote at any of them during election day. Legal amendments are required in these cases.

Conformity of e-voting solutions with national principles for democratic elections (national norms include the international standards of Article 25 ICCPR and Article 3 of Protocol № 1 to the European Convention on Human Rights) has been examined by the supreme courts in *Germany*, *Austria*, *Estonia*, *Switzerland*, and *France*, amongst others.[31] Concerns about foreign interference in elections have more recently led to closer scrutiny of the security (and thus, compliance) of digital solutions, other than e-voting, used in electoral processes, namely voter registers and registering or results transmission and calculation systems, as was the case in *Germany* and *the Netherlands* in 2017.

---

29. 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, as is the case in Romania.

30. Three days after the election, a final scrutiny of the paper votes sent in by each polling station is carried out, in which the Electoral Boards are assisted by a computer application that facilitates their work.

31. For an international comparative view, see Driza Maurer, Barrat (eds), E-Voting Case Law – A Comparative Analysis, Routledge 2015, 2017. In addition to the European countries mentioned, case law in India, Brazil, Mexico, the USA, Australia, Argentina and Venezuela is also discussed.

When digitising processes, an initial question that arises is how should the digitised process look: should it mimic the traditional, paper-based process, or can it introduce new disruptive features necessary for compliance and which are made possible by new technology? So far, mimicking has prevailed. For example, from an equal-suffrage perspective, an e-voting channel is not allowed to offer more or different possibilities to voters than a traditional channel (see standard 5 of the Recommendation CM/Rec(2017)5). However, another logic, centred on achieving objectives as opposed to achieving formal equality between solutions based on different technologies, has been employed and looks more appropriate. It focuses on principles that need to be respected/applied and considers the specificities of the technology employed. For instance, specific e-voting vulnerabilities and threats recommend that individual verifiability and universal verifiability are introduced to ensure respect for the principle of free suffrage (see standards 15 ff of the Recommendation CM/Rec(2017)5). Now, individual verifiability in e-voting enables the voter to verify their own vote, which is a totally new feature that does not exist in paper-based voting. Also, multiple voting is allowed specifically for internet voters (in some countries), to counter the family voting risk, which is present in all distant voting, including internet one. Another example is the specific design of an e-voting system to enable, as far as is practicable, persons with disabilities and special needs to vote independently. Yet another is the requirement that an e-voting system shall advise the voter if he/she casts an invalid vote (standard 14 of the Recommendation CM/Rec(2017)5). Again, this is not possible with paper voting: in this case, e-voting offers an advantage that helps to better ensure the right to free suffrage.

To conclude, the digitisation of documents and processes plays a significant role in supporting elections in many Council of Europe countries by enabling accelerated and uniform data processing. Every phase of the electoral cycle is supported by digital tools. Their introduction and expansion are continuous and may lay the groundwork for later introduction of other new technologies.

Biometry

Biometry introduces the opportunity to capture and save in electronic format some physical characteristics (iris, fingerprint, facial recognition, etc.) that should enable the unique identification of a person. Traditionally, unique identification is ensured by procedural rules and is based on voters' registers. By augmenting electoral rolls with biometric data, the aim is to ensure the unique identification of voters and prevent multiple voting. On election day, voters' biometric characteristics are captured and compared to biometric information stored in databases. Biometry in elections has been used mainly in countries in South America or Africa. With very few exceptions, the Council of Europe member states do not consider biometry in elections. Data protection, vote secrecy as well as voter disenfranchisement due to errors in biometrical identification (false accept and false reject) are amongst the main reasons for not using biometry in elections in Europe so far. A 2018 French Senate report suggests considering unique identification of voters by introducing biometry.

The use of biometry in elections raises questions of compliance with Article 3 of Protocol № 1 to the European Convention on Human Rights. How unique and permanent are biometrical characteristics to ensure the right to vote over time? Is it easy and quick to collect biometrical information and authenticate the voter during the vote? Is the collection and use of such characteristics accepted by voters? Secure data storage (data secrecy protection) and system security must be ensured.

Blockchain

Blockchain is an immutable time-stamped series record of data that is distributed and managed by a cluster of computers. Its main characteristics are decentralisation, transparency and immutability.[32] The transactions being recorded across many computers ensure that any record cannot be altered retroactively, without the alteration of all subsequent blocks.

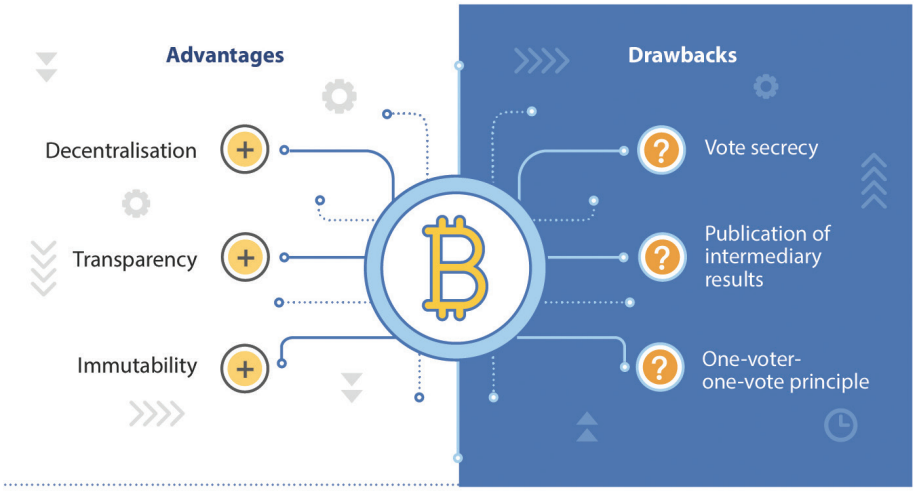
A few trials with blockchain voting have taken place at a local level.[33] Blockchain voting claims many advantages over traditional, centralised, paper-based voting systems. However, most of its properties (for example, electronic identification, digital signatures to guarantee the integrity of the data, strong cryptography, voter verifiability, and multiple voting possibilities) are not exclusive to blockchain and are also present in "traditional" verifiable e-voting. Blockchain voting introduces at least one specific feature: any information processed, via computing or data storage, is shared across multiple nodes (decentralisation). In a decentralised voting system, a set of entities must agree on how a vote has been cast before recording it. This means that there is no single entity taking control: it is not only the organiser of the poll, the EMB, that validates a vote, it could also be various accredited institutions (for instance, the Council of Europe, political parties, or local councils). This offers the advantage of protection against internal threats: allegedly, even a corrupt government cannot forge the votes. Once a vote has been recorded, it cannot be removed or altered as blockchain claims to be immutable. If there are enough nodes (in the cluster), it is claimed that the system is hacker-proof. Voters' identities are anonymised and the votes are allegedly secret. This is questionable as a person's identity can be tracked down using public address information and IPs. Other issues relate to interoperability, costs, etc.

Blockchain is increasingly used for processes where unalterable, persistent, and searchable records or transactions, contracts and official documents are required. Administrations use it for official registers of land, or official transactions, etc. One can envisage that administrations that embrace blockchain may be tempted to use it in the electoral cycle as well; for instance, to keep registers of voters, parties, etc. So, if the Civil Register is based on blockchain, then the extracted electoral register will probably be kept the same way. Introducing blockchain to handle one element of the electoral cycle may affect the whole cycle.

32. Source Wikipedia, https://en.wikipedia.org/wiki/Blockchain

33. For example, the city of Zug in Switzerland conducted a mock blockchain i-vote on 25 June-1 July 2018. See the evaluation at http://www.stadtzug.ch/dl.php/de/5c00ff8dbd830/eVoting_Final_Report_ENG.pdf

Use of blockchain in electoral processes



Blockchain raises several conformity issues with respect to Article 3 of Protocol № 1 to the European Convention on Human Rights, *inter alia* on vote secrecy (as data posted on the blockchain stays there), on non-publication of intermediary results (as the number of votes for each candidate is known before the voting is finished); on security; user-friendliness (as a substantial waiting period is required until a transaction or vote is concluded); respect of the one-voter-one-vote principle (as computational power is important for decision-taking in blockchain), etc.

Cloud computing

Cloud computing is the on-demand availability of computer system resources, especially data storage and computing power, without direct active management by the user. The term is generally used to describe data centres available to many users over the Internet.[34] There are public as well as private clouds.

Organisations, like business, are inclined or have already transferred their IT to the cloud as it is supposed to be cheaper and more secure than maintaining in-house capacities. This is challenging when it comes to critical systems like elections, where the authorities should have the upper hand and preferably – as conventional wisdom would have it today – in-house IT expertise and solutions.

The cloud may introduce new vulnerabilities into the electoral system; for example, the security of sensitive documents and processes, secrecy and privacy, accountability or interoperability (namely the possibility to retrieve the data or transfer it to another cloud) and as many threats of attacks, while the investigation

34. Wikipedia, https://en.wikipedia.org/wiki/Cloud_computing

of irregularities and forensics becomes more complex. The use of cloud computing for documents and processes of the electoral cycle has not been much thematised. Its actual use and the ensuing conformity questions (secrecy, security, interoperability, etc.) need further investigation.

Artificial intelligence

Artificial intelligence (AI) refers to a wide range of methods, both current and speculative.[35] It refers to systems that display intelligent behaviour by analysing their environment and taking action – with some degree of autonomy – to achieve specific goals.[36] The AI field draws upon many fields. The traditional goals of AI research include reasoning and decision making (knowledge representation, planning, scheduling, search, optimisation), learning (machine learning, neural networks, deep learning, decision trees, etc.) and robotics (embodied AI; the ability to move and interact with the physical world). So far, AI solutions are domain specific.

AI may have an impact on new technology solutions used in elections. For instance, it will potentially be used to conduct cyberattacks in a way that is even more sophisticated and difficult to predict than now "including more able to pursue highly customised objectives, and to adapt in real time".[37] This should be taken seriously by EMBs. At the same time, it is also expected that AI will be trained and used for cyber defence. AI may also be envisaged in training and education, or in dispute resolution issues. It may be interesting for information-retrieving purposes.

The main issues related to AI include data issues and explainability. AI systems need to process a lot of data to perform well and are only as good as the data that are fed to them. If the training data are biased (for instance, not inclusive enough), so will the AI trained on it be and consequently its decisions will be unfair. There is one important caveat though: the principle of open data does not apply to all kinds of data gathered in elections, which renders the development of AI solutions for elections more difficult. Indeed, the opposite is true as, for example, detailed information on participation and on the content of the vote are covered by the secret suffrage requirement. Explainability relates to the opaque nature of some AI: it is impossible, even for their engineers, to understand how they make decisions. There is growing national and international consensus that AI systems must be designed so that their decisions can be explained, and humans remain accountable.[38]

35. European Parliamentary Research Service (2019) "How artificial intelligence works", "Why artificial intelligence matters". See also Wikipedia, https://en.wikipedia.org/wiki/Artificial_intelligence

36. European Commission, indep. High-level expert group on artificial intelligence, "A definition of AI: Main capabilities and disciplines", 8 April 2019

37. UN High level panel Report, *The age of digital interdependence*, June 2019

38. Recommendation 3C of the UN High level panel Report, *The age of digital interdependence*, June 2019; US *Algorithmic accountability act of 2019*; German Government *Strategie Künstliche Intelligenz der Bundesregierung*, Nov. 2018; Cedric Villani (France) Report *For a meaningful artificial intelligence. Towards a French and European strategy*, of March 2018

b. Electoral cycle perspective

I. Legal framework

This part of the electoral cycle includes the design and drafting of all legislation and regulation of elections at all levels of government and of all types, including formal and material law and even codes of conduct and other instruments that may have a direct or indirect impact on elections. Not all of these elements are initiated or drafted by the EMB, so it is also important for the EMB to have a good overview and understanding of all regulatory elements to be considered in the electoral cycle. This is where new technologies may help, for instance, in preparing, organising and retrieving information.

Another aspect to this issue is that legislation should regulate the use of new technologies in the electoral cycle. So far, it has proved difficult to write regulations that comply with higher-level principles, as shown in the decisions of the constitutional courts of Germany and Austria on the conformity of e-voting regulations. It is unclear how the legal principles apply to new technologies and what the content of a compliant regulation should be. Principles like legality or the legal certainty of the electoral law are challenged by the complexity of new technologies and their rapid evolution.

One difficulty relates to concepts whose content and scope may be different in the digital world as compared to the analogue one. In an analogue world, election security and controls, for instance, are considered in a rather static way, as well-defined products and processes, whereas in a digital context, they must advance daily to respond to evolving vulnerabilities and threats, and face new risks. Some compare this to an arms race. This aspect should be reflected in regulation, but how? In the analogue world, for instance, EMBs are responsible for security except in exceptional cases such as *force majeure*. How do we define their responsibility in a digital context? It is easy to accept *force majeure* in low tech contexts. Is hazard in software (with reference to AI) acceptable? As new technologies evolve through trial and error, what should an EMB ensure, namely what positive obligations arise from its task of ensuring conformity with Article 3 of Protocol № 1 to the Convention throughout the electoral cycle?

The answers are far from trivial. Constitutional courts (for example, in Germany and Austria), parliament, government and watchdog organisations (for example, in the Netherlands, Norway or France) have recognised the shortcomings of existing regulations, for instance, for e-voting. Inherited from the 70s, 80s, and 90s, such regulations should evolve to take account of the newest technologies. In a few cases (Belgium, Estonia, Switzerland), the regulator has upgraded them or introduced new ones. Their conformity is tested in practice and it appears that such regulations need to continue to evolve (an example is the Swiss 2019 i-voting transparency exercise and lessons learned on verifiability, transparency and certification).[39]

39. Driza Maurer, Ardita (2019), *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

Guidance from the Council of Europe Recommendation CM/Rec(2017)5 has been important to countries in their regulatory efforts for e-voting. The most recent wave of questions has not yet been thoroughly discussed, including the following: control of the vote-verifying mechanisms, evaluation of trust assumptions which are necessarily present in verifiable e-voting, follow-up to transparency (for instance, what happens after the source code is published), etc.

Of all the new technologies used in the electoral cycle, e-voting seems to have received the greatest attention, from a regulatory perspective. Other digital solutions used in the electoral cycle are regulated, at best, from an IT management perspective only. Attempts by EMBs to introduce/upgrade such regulations often meet with resistance.[40] However, things are changing, in particular since the thematisation of interference by foreign countries after the US 2016 presidential elections and the suspected hacking of some e-backed solutions. Recent examples from the 2017 elections in the Netherlands (counting and tabulation software) and Germany (results transmission software) show that processes vital to the outcome of the election face challenges similar to those of e-voting and should be better regulated. Their conformity with Article 3 of Protocol № 1 to the Convention and national electoral principles should be better investigated.

Conformity with Article 3 of Protocol № 1 to the Convention requires that digital solutions also implement/comply with some conditions: gradual introduction of new technologies, accountability (certification, audits), distribution of responsibilities, transparency and observation, reliability and security, and interoperability, amongst others. The replies to the CDDG questionnaire show that countries welcome guidance from the Council of Europe. For instance, Recommendation CM/Rec(2017)5 on e-voting is considered important by countries including those that allow the e-casting of the vote (Belgium, Estonia and Switzerland) and those who only practice pure e-counting (Czech Republic, Denmark or Hungary). The countries' replies suggest that further discussion at the regional level is needed on issues of cybersecurity in elections, verification of the vote, digital identity, contingency procedures in case of interruption of communications, and that these issues should receive more attention at a regulatory level.

II. Planning and preparation

The EMB oversees the detailed steps of the electoral cycle: election calendar, recruitment and training of staff, logistics and security, national or regional electoral policies, electoral services, procurement for outsourced services, recruitment and training of electoral staff, etc. IT support adapted to its needs is used for this purpose.

The main issue here is the extent to which these solutions are hacker-proof (security), the extent to which the electoral cycle processes are dependent on them and whether or not back-up solutions are foreseen.

40. An example is the discussion around federal regulation of e-counting solutions in Switzerland and the initial reticence, namely of cantons, who are in charge of introducing, operating and monitoring these solutions.

III. Training and education

The EMB usually conducts voter and civic information and education. It supports access for all, promotes equality and equity policies and practices, and may provide electoral research facilities. In addition to voters, it hires and trains temporary electoral staff. The EMB provides observer accreditation and regulates their conduct. It trains political parties' and candidates' poll watchers. EMB activities extend to the media: it provides media access, regulates the conduct of the media during elections, and regulates opinion polls.

IT is used to support such activities. The same issues identified under planning and preparation apply here as well.

IV. Registration

As mentioned under digitisation, there are mainly two types of registers: electoral or voters' registers and parties' registers. During the vote, the use of voting rights (the fact that a person voted) is also registered. They are probably all digitised in all Council of Europe countries.

Voters' registers include voters living in the country, voters living abroad who are eligible to vote and, in some cases, foreigners established in the country. The EMB also registers political forces (parties, movements, etc.). Before each election, it receives and validates the nominations of candidates. In addition, it may oversee political party pre-selections or primaries.

With respect to compliance with Article 3 of Protocol № 1 to the Convention, one issue faced by all registers is the unique identification of individuals, namely of voters and candidates. Unique identification serves the purpose of ensuring equal suffrage (one person, one vote) as well as the respect of electoral rules on candidacy. In analogue paper-based systems, individuals are identified manually: the procedure is cumbersome and prone to errors in verification. In a digital world, e-backed solutions offer the advantage of quick verification and effective prevention of multiple voting or multiple candidacies. A solution under consideration is unique e-identification. Estonia uses e-IDs for voter authentication. In some countries without e-IDs, attempts have been made to use alternative unique identifiers, such as social security numbers, for instance, for identifying candidates. Initially, this was fiercely resisted by data protection watchdogs. Data protection concerns prevailed over respect for electoral principles (candidacy rules or one person, one vote). More recently, data protection watchdogs have started to accept such use. In parallel, e-IDs are becoming more common. Allegedly, they facilitate transactions in all areas of life. Vote and participation secrecy remain important and should be considered attentively as use of e-IDs and other e-identification tools becomes routine.

V. Electoral campaigning

Use of new technologies in electoral campaigning refers mainly to opinion formation. As mentioned previously, use of new technologies for opinion formation issues is outside the scope of this paper.

VI. Voting operations

This phase refers to the election process, from the opening to the closing of the vote and subsequent counting, verifying and publishing of results. Several digital solutions, including e-identification of voters, e-voting, e-counting, e-transmission of results can be used during this phase. Questions of conformity were discussed above, under technology perspective/digitisation.

VII. Election results

In addition to collecting, tabulating and publishing results (see above), EMBs also use digital solutions to conduct audits and verifications of the correctness of the results. There exist tools that check the plausibility of results, that is, identify electoral irregularities by statistical methods.[41] Statistical methods evaluate probabilities of correctness of results based on data from previous elections. They must be "fed" with data from current and previous elections. As for AI, the quality and quantity of such data are crucial for these methods to function optimally.

EMBs may also act as a dispute-resolution authority. Digital solutions may be used to retrieve and process information. There is no talk of predictive justice here; however, such tools may be interesting and help EMBs take make correct and swift decisions. They may also be used to help voters better understand their rights and how to defend them, thus improving access to justice for complaining users (voters, parties, etc.). In all these cases, attention should be paid to the conformity of the solution specifically with free and secret suffrage and with the right to an effective system of appeal.

VIII. Post-election duties

Such duties include the deletion or archiving of the election's data, work to update information and tools, reviewing and evaluating the adequacy of the electoral framework and the EMB's own performance, and advising the government and legislature on electoral reform issues. The same observations for planning and preparation apply to the digital tools used here. Furthermore, vote and participation secrecy should be respected.

---

41. European Commission for Democracy through Law (Venice Commission), 2018, "Report on the identification of electoral irregularities by statistical methods", CDL-AD(2018)009

3. SYNTHESIS AND TRANSVERSAL ISSUES

This quick overview shows that the most widespread and necessary technology is digitisation. It is the founding layer of any other new technology, like biometry, blockchain, cloud computing, or artificial intelligence.

It is important that digital solutions used in the electoral cycle comply with the principles and conditions for democratic elections. The question has been dealt with in some depth with respect to e-voting. The compliance of digital solutions used in the electoral cycle, other than e-voting, has so far gone unnoticed. Recent developments show that the use of such solutions must be carefully planned and regulated. Requirements for sensitive documents and processes may be aligned with the Recommendation CM/Rec(2017)5 requirements for e-voting.

Some questions are transversal: they are of interest to all digital technologies and all phases of the electoral cycle. Such questions include cybersecurity, data protection, contingency procedures or public-private co-operation. Existing Council of Europe instruments already deal with them. However, elections remain a case apart, to which stronger requirements such as data protection or cybersecurity may apply. Countries' responses to the CDDG questionnaire suggest that work at a regional level is necessary, especially on cybersecurity, verification of the vote, digital identity, and contingency procedures in case of interruption of communications.

Data protection is such a transversal issue. It is regulated by the Council of Europe Modernised Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108+). At the EU level, the main legal instrument is the (EU) 2016/679 General Data Protection Regulation (GDPR). Council of Europe Convention 108+ and GDPR were developed in parallel and are consistent with each other. GDPR amplifies some principles of Convention 108+. Data used in elections or linked to political opinion are qualified data, whose processing should only be allowed if appropriate safeguards are enshrined in law (Article 6 of the Convention 108+). However, for those in charge of elections, it is not clear how the appropriate safeguards should look. The interplay between different instruments and the specificities of elections should be considered. Combined expertise is required; for instance, the use of cryptography may be an important measure to protect some of these data.

Another transversal issue is cybersecurity. The Budapest Convention on Cybercrime regulates an important aspect of cybersecurity, which is co-operation between countries to prosecute offences against free, fair and clean elections. Other aspects are regulated at the national level, for instance, by regulations on the cybersecurity of critical infrastructures. Elections are being classified as critical infrastructure. Their security is particularly important. So is planning to deal with attacks (corruption of data, interruption of service, etc). Examples of administrations whose work was compromised, for example, by ransomware (Baltimore, May 2018) show what could go wrong in elections and how critical processes could become the target of politically or financially motivated hackers, etc.

Public-private co-operation is yet another important transversal question as digital solutions and their control are mainly provided by the private sector. Procurement conditions should reflect requirements that are important for compliance of the solution with Article 3 of Protocol № 1 to the European Convention on Human Rights. It is important to clarify responsibilities. Political responsibility for the use of digital solutions in elections should lie with the EMB. It should be clear from the beginning of the co-operation between the EMB and private providers how non-compliance questions will be addressed.

4. SELECTED REFERENCES

Council of Europe, Committee of Experts (MSI-AUT), *Draft Recommendation of the Committee of Ministers to member States on the human rights impacts of algorithmic systems,* 26 June 2019.

Council of Europe, *Convention 108+, Convention for the protection of individuals with regard to automatic processing of personal data* (June 2018).

Council of Europe, Consultative Committee of the Convention for the Protection of Individuals with regard to the processing of personal data, *Report on Artificial Intelligence. Artificial intelligence and data protection: challenges and possible remedies*, of 25 January 2019.

Council of Europe, Cybercrime Convention Committee (T-CY), *Guidance note № 9, Aspects of election interference by means of computer systems covered by the Budapest Convention, 08.07.2019.*

Council of Europe, *Declaration by the Committee of Ministers on the manipulative capabilities of algorithmic processes*, 13 February 2019.

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

European Commission, *Free and Fair Elections. Guidance Document. Commission guidance on the application of Union data protection law in the electoral context.* A contribution from the European Commission to the Leaders' meeting in Salzburg on 19-20 September 2018.

European Commission, High-level expert group on artificial intelligence, *A definition of AI: main capabilities and disciplines,* 8 April 2019.

European Commission for Democracy through Law (Venice Commission) *et al.*, *Joint Report on Digital Technologies and Elections,* 21-22 June 2019.

IDEA, *Cybersecurity in elections. Models of interagency co-operation*, 2019.

IDEA, *Electoral Management Design,* Revised Edition, 2014.

OSCE/ODIHR, *Handbook for the observation of new voting technologies,* 2013.

UN Secretary General's High-level panel, *The age of digital interdependence*, June 2019.

Digital solutions are increasingly used in elections. Their security has attracted much attention in the recent years as it impacts the integrity of elections. The legislator has the important burden to introduce regulations ensuring that only digital solutions which comply with constitutional principles can be used in elections. This is not an easy task as the field is still experimental. The two studies presented here raise legal questions, draw upon past experiences in several countries and suggest possible approaches. This publication will be of interest to legislators and executive authorities, namely Election Management Bodies, that are invited to decide on the use of digital solutions in elections.

www.coe.int

The Council of Europe is the continent's leading human rights organisation. It comprises 47 member states, including all members of the European Union. All Council of Europe member states have signed up to the European Convention on Human Rights, a treaty designed to protect human rights, democracy and the rule of law. The European Court of Human Rights oversees the implementation of the Convention in the member states.

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE