# New technologies in the electoral cycle.
# Guidance from the Council of Europe

Ardita DRIZA MAURER

Jurist, independent consultant, Switzerland

CDDG/GT-DT Expert

*v.2*

(v.2 January 2020, updated March 2020)

This is a reworked version of the report dated Sept. 2019 submitted to CDDG

**GENERAL DISCLAIMER**

The opinions expressed here are the author’s own and do not necessarily reflect the views of the Council of Europe.

# 1. APPROACH AND DEFINITIONS

## a. Introduction

For the biennium 2020-2021, the European Committee on Democracy and Governance (CDDG) has received the specific task of developing standards on new technologies used at the different stages of the electoral process, including voter registration, transmission and tabulation of results, etc. (specific tack ii). This task is dealt by the working group on democracy and technology (GT-DT). Standards may take the form of a Committee of Minsters' recommendation or guidelines, or both, according to the mandate. The GT-DT is asked to provide a clear indication of the best-suited standard-setting instrument to be adopted by the Committee of Ministers and to identify key recommendations. Protection of opinion formation of voters from manipulation (informational environment, social media, fake news, opaque algorithms, etc.) will not be discussed as it is subject of work in other forums, at the Council of Europe and in other organisations.[1]

As guardian of the values enshrined in the ECHR and its protocols, the Council of Europe (CoE) has the core mission of overseeing the implementation of ECHR in countries of the region, including in election related activities. Pursuant to art. 3 of the additional (first) Protocol to ECHR (hereinafter P1-3 ECHR)[2] and case law of the ECtHR, the EMB (i.e. the State) has the positive obligation to make sure that all activities led by it within an electoral cycle comply with the right to free elections, including those backed by new technologies. These last ones should also respect related rights such as freedom of expression, non-discrimination, etc. This report focuses on respect and implementation of P1-3 ECHR, 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 (e.g. 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.

New technologies improve and facilitate several aspects of elections, but also bring challenges and risks with them. Their use may increase efficiency and speed, help avoiding errors associated with manual work, etc., but they are also complex, subject to rapid change and may open the door to unpredictability and even to attacks against the electoral process. It is important for EMBs to take informed decisions on the use of new technologies so that it's done in a secure way, and elections benefit from the advantages whereas risks are minimized and under control so that EMBs can guarantee overall secure elections. To do so, multidisciplinary work is required. The required competences are not readily available and need to be developed. Setting standards at the CoE level means achieving harmonized interpretation of principles and regional consensus. In addition, CoE can mobilise multidisciplinary international expertise for the purpose of developing standards. To be noted, CoE is the only international organisation, at the regional level, with the mandate to develop principles and standards for elections. Through its Centre of expertise in good governance, CDDG has furthermore the potential to assist member states with focused expert advice, whenever necessary (of course

[1] See e.g. European Commission for Democracy through Law (Venice Commission) and the Directorate of information society and action against crime of the Directorate general of human rights and rule of law (DGI), 2019, "Draft Joint Report on Digital Technologies and Elections", of 7 June 2019, CDL(2019)002.

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

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

upon agreement to develop the Centre in this direction and mobilise expertise available). All this would contribute to implementation and respect of P1-3 ECHR when using new technologies.

How to deal with the task of developing standards on new technologies and the different stages of the electoral process? This Chapter presents the approach and the definitions of the main terms of the research, namely the electoral cycle and the new technologies used throughout the electoral cycle. Chapter 2 overviews first, the main features, uses and issues of some new technologies implemented or considered for use in the electoral cycle. Secondly, it looks at the different elements of the electoral cycle to find out which new-technology solutions are already used and what we know about their conformity with P1-3 ECHR. Chapter 3 offers a synthesis of the main questions and issues associated with new technologies and their use in the electoral cycle. Finally, Chapter 4 considers standard-setting by CoE and possible approaches by GT-DT/CDDG of the question of elaborating guidance on the use of new technologies in the electoral cycle.

The report builds on previous work at the CoE, namely on work in the e-voting field (Recommendation 2017/5 on standards for e-voting, hereinafter Rec(2017)5), including the first self-evaluation of the implementation of Rec(2017)5 by 30 countries that replied to a short questionnaire distributed by the secretariat in 2019. Also work by Venice Commission on ICT in elections as well as work at CoE in related areas such as electoral assistance, cybersecurity (Budapest Convention), data protection (Convention 108+) as well as relevant work by other organisations, namely the EU, OSCE/ODIHR, international IDEA, etc., are taken into account.

## b. Electoral cycle

From the perspective of the Election Management Body (EMB), i.e. the State authority in charge of organising elections, an electoral cycle[4] encompasses all steps and processes that fall within the extent of its functions, responsibilities and powers and that are necessary for an election or vote to take place. The cycle further implies that the process is reiterated election after election. The main phases of an election's cycle are the following (they do not necessarily follow sequentially):[5]

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).
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.

**The Electoral Cycle**

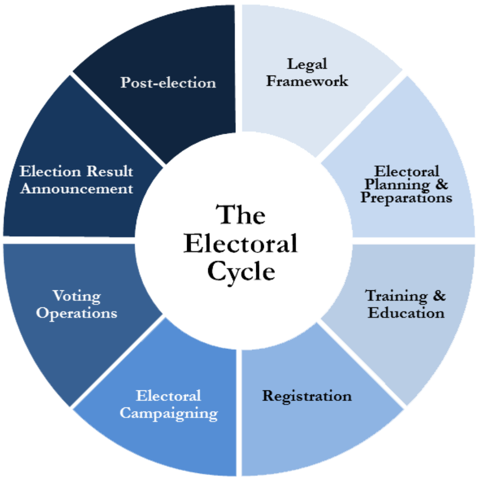

Image source : IDEA

The conduct of direct democracy votes involves similar steps as well as 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 phase (no. 4 above). After that, like in elections, the EMB informs voters, plans and conducts the vote. In this document, the term election/electoral cycle refers to both elections and direct democracy votes.

## c. New technologies

For our purpose, "new technologies" refers to "digital solutions" employed in the electoral cycle. It covers different solutions, including digitization of documents and procedures, the use of biometry, blockchain, cloud

[4] We refer mainly to the election cycle as defined by IDEA in *Electoral Management Design, 2014: 12; 16; 75-77*, with minor changes and complements.
[5] The electoral cycle was conceptualized 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 plan 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

computing or internet of things, among others. Use of artificial intelligence is being discussed, also beyond opinion formation issues.

Digital technologies store and handle information digitally (a series of ones and zeros or on and offs) and are not observable or understandable by the layman. More complex ones, such as artificial intelligence, are trained to draw meaning from digital data and may evolve so that their detailed functioning may not be understood even by the engineers who built them. In addition to being complex, digital technologies also evolve very rapidly. Thus, they profoundly differ from paper-based solutions.

This report focuses on "new technologies" that are already in use (digitization, biometrics) and those whose use may increase/be considered in the future (blockchain, cloud computing, artificial intelligence). We consider their use throughout the electoral cycle, to the notable exception of opinion formation (electoral campaigning) and financial aspects which are outside the scope of this document.

## 2. QUESTIONING THE USE OF NEW TECHNOLOGIES IN ELECTIONS

### a. Technology perspective

Below we consider some new technologies used in the electoral process and highlight main questions of conformity with P1-3 ECHR.

#### *i. Digitization*

Digitization is the first layer, at the foundation of all "new technology": it is the conversion of text, pictures, or sound into a digital form that can be processed by a computer. Its main advantage is to allow for computer treatment of information, i.e. error-free, efficient, quick, etc. Almost all countries in the region have digitized the key data and processes.[6]

Digitized data include electoral registers, registers of candidates, voting registers, collection of other basic data in electronic format, results in electronic format, etc. Digitized processes include e-registering, e-identification of voters (e-pollbook), e-voting (both on voting machines in polling stations and over internet), e-counting (programmes that register and calculate results and may also allocate seats), programmes that establish statistics and draw any other information on elections, e-transmission of preliminary and/or final results e.g. from polling stations to a central unit, etc. Digitization of processes is more challenging when they transit over the internet. In some countries, the digitized data and processes are grouped in election information systems.

When digitizing processes, one dilemma is to decide how should the digitized process look like: should it mimic the "traditional" process (as most solutions do so far) or can it be a new disruptive process that takes advantage of the opportunities offered by the new technology? So far, mimicking has prevailed. For example, from an equal-suffrage-perspective, an e-voting channel is not allowed to offer more/different possibilities to voters than a traditional channel (standard 5 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. It focuses on principles that need to be protected and takes into account the specificities of the different technologies employed. For instance, e-voting being exposed to specific risks (compared to paper-based voting), *individual verifiability* is required to ensure respect for the principle of free suffrage (standards 15 ff.). Individual verifiability enables the voter to verify her own vote, which is a new, disruptive process compared to paper-based voting. *Multiple voting* is allowed in internet voting and not in paper-based voting (in some countries), to counter the specific risk of family voting that is present when doing internet voting. Universal suffrage commands that an e-voting system be designed, as far as is practicable, to enable

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

*persons with disabilities and special needs to vote independently* – an advantage specific to e-voting. Free suffrage again commands that the voting system shall *advise de voter if he/she casts an invalid vote* (standard 14) – a possibility specific to e-voting.

The replies to the CDDG questionnaire on implementation of Rec(2017)5 distributed in 2019, offer an overview not only on e-voting but, also more broadly, on the digitization of data and processes of the electoral cycle and provide indications on trends. We summarize them in the following paragraphs.

E-voting is the most advanced example of use of new technologies in the electoral cycle, for two reasons mainly: first, e-voting covers the most sensitive process of an electoral cycle, i.e. the actual vote and the results of an election, so the technology used is subject to particular scrutiny. Second, e-voting is not only the digitization of the voting and counting, but it, ideally, also implies and requires that all involved documents and processes also be digitized so that information and transactions can flow without media discontinuity.

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 Internet from an uncontrolled environment (hereinafter i-voting). E-casting implies e-counting. There is also the pure e-counting, i.e. of paper ballots which requires the use of optical scanners to digitize the paper ballot and then proceed to the counting.

E-casting of the vote is practiced in a few countries, as shown by replies to the questionnaire, including *Belgium* (EVM for all kinds of elections and referenda); *Bulgaria* (EVM only for national and EU elections as well as election of president and vice-president of the Republic of Bulgaria but not for referenda); *Estonia* (i-voting for all national elections but not for local referendums 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* (for local referenda only); *Russian federation* (EVM for national and regional elections); *Switzerland* (i-voting for federal, cantonal and communal votes and elections; however *de facto* suspended since June 2019).

E-counting via optical character recognition technology is practiced in *Hungary* (for preliminary results only), *Latvia, Malta* (in May 2019 MEPs and local councils elections), *Norway*, *Switzerland* (some cantons scan and e-count paper ballots in referenda), the *United Kingdom* (*England* in 2000, 2004 and continuing in local and national elections and *Scotland* in 2007 local and national elections; significant errors were found in the ballot design; e-counting was used again in 2012 and 2017 local elections without problems; the counting time of the ballot papers [Single Transferable Vote system] has been reduced from three/four days to a matter of hours) and in the *Russian Federation*.

The replies to the questionnaire show that e-casting of the vote is envisaged in *Azerbaijan* (next municipal elections), in *France* (a Senate 2018 report recommends use of i-voting in consular elections in 2020 and in parliamentary elections in 2022; the French Government recently approved the internet voting solution for the 2020 election); in *Romania* (the Permanent Electoral Authority is considering e-voting, however any implementing may not begin before the end of 2020 due to mistrust of political actors and administrative institutions); in *Serbia* (a possibly upcoming law on referendum and popular initiative considers the e-initiative as a first test of e-voting); in *Ukraine* (a law on national and local referendums is prepared which will consider the e-voting option); in the *United Kingdom* (a non-binding trial took place in May 2019 in a local election featuring an end-to-end verifiable system, according to its authors, comprising touch-screen computer 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. This trial took place in a context where the Welsh and Scottish governments have proposed pilots of e-voting in local elections).

Electronic casting of the vote has been partially or totally suspended or abolished in the following countries: in *Bulgaria* (in 2019, the Parliament abolished e-voting for local elections due to the complexity of such elections and related financial cost of e-voting); in *Finland* (after the 2008 municipal election test and identified problems); in *France* (since 2008, a moratorium has suspended any extension of EVMs to new communes; i-voting was cancelled at the last national elections but is expected to be used again in 2020 and 2022); in *Germany* (the Federal Constitutional Court decision of 3 March 2009[7] declared the Federal Ordinance on Voting Machines[8] to be incompatible with the principle of open [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); in *Ireland* in 2008; in *the Netherlands* (in 2006, following decades of e-voting, the EVM came under heavy criticism for lack of security and auditability; since 2008, voting is held using only paper ballots); in *Norway* (after trials in 10 and 12 municipalities resp. in 2011 and 2013, i-voting was discontinued because of lack of political will to establish it as a regular channel); in *Switzerland* (since mid-2019 internet voting has been *de-facto* suspended as there are no i-voting systems that fulfil the legal requirements); in the *United Kingdom* (after trials in local elections in England between 2002 and 2007, e-voting was discontinued mainly because risks were considered to outweigh advantages, complexity and transparency issues and because a clear vision, strategy, effective planning, cost-effectiveness, system certification were lacking).

E-voting has been considered but not launched for political elections in *Austria* (after a Constitutional Court decision of 2011 saying that the electoral commission must understand all steps and procedures of i-voting without assistance from technical experts), the *Czeck Republic*, *Danemark*, *Finland* (a report concluded end 2017 that risks of i-voting currently outweigh benefits), *Latvia* (some discussions in parliament and society show however that introduction of i-voting is again considered although it is not popular concept), *Spain* (the question has been raised only for the Spaniards abroad). The main arguments against the introduction of e-voting are security, complexity and high costs.

Outside e-voting, the digitization of documents and processes of the electoral cycle is widespread. Here is a brief overview resulting from the answers to the questionnaire alone:

- Basic data on electoral districts, municipalities, voting districts, election authorities, preparation and publication of candidate lists, and preparation of ballots layout are reported by *Finland, Hungary, Latvia*.
- Services/processes before voting day including:
  - e-services for electors to find and to change their polling station (*Hungary*), to apply for postal voting (*Latvia*), to check and amend their electoral details (*Ireland*) or to register for voting abroad (*Spain*);
  - signature collection for new parties wishing to stand for elections in *Denmark* (the Danish Parliament decided in 2019 to procure a redesigned system);
  - signature collection for national/local referenda (*France*).
- Services/processes during and after voting day include:
  - the electronic *journal* with all important figures and events (*Latvia*) and may also include e-poll books;
  - electronic data exchange among polling stations, ensuring the possibility for voters to vote at any polling station during early voting days (pilot project at the 2019 European Parliament Election in *Latvia*);
  - transmission of provisional and/or final voting results from the manual counting at polling stations to central entities where they are consolidated, counted and published, as the case may be

[7] BVerfGE 123, 39

[8] 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).

    (*Austria, Azerbaijan, Croatia, Cyprus, Czech Republic, Danemark, 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 digitized documents to be used almost everywhere in the region are registers: registers of voters and candidates, registers that keep track of those who already voted during an election (use of voting rights) (everywhere where *e-casting* of the vote is used, as well as in *Finland*, *Hungary*, *Latvia*, *Norway*, *Serbia*, *Slovenia*).
- Services/processes after voting day also include:
    - Solutions to *check results.* This goes from applications for identifying arithmetical errors regarding the data written down on the paper-based election protocols (any mismatch between figures is flagged by the application; as a precautionary measure, the software may be designed not to allow for immediate data transmission in cases where figures do not reconcile like in *Romania*) to statistical audit methods for checking the plausibility of results (these are mainly used in the *USA*);
    - final scrutiny of results in *Spain*: three days after the election, a final scrutiny of the votes in paper sent by each polling station is carried out, in which the Electoral Boards are assisted by a computer application that facilitates their work.
    - registration and publication of data on voter turnout, statistics and information: *Croatia, Finland,* among others.

Plans for extension of the use of IT in the electoral cycle are reported in several countries, namely *Denmark* (an Election management systems is expected to be deployed in 2020), *France* (e-signature gathering for referendums), *Finland* (Election Information System or EIS to be introduced), *Ireland* (electoral register modernisation project currently underway; among others, a national roll out of online registration is examined), *Latvia* (intention to introduce an electronic voters' list for polling stations in the next municipal and parliamentary elections to give the possibility to vote at any of them during election day. Legal amendments are required).

To conclude, digitization of documents and processes plays a significant role in supporting elections in many CoE countries by enabling accelerated and uniform data processing. Every phase of the electoral cycle is supported by IT tools. The construction and expansion of digital solutions is continuous. Digitization is considered a solid basis for later introduction of other new technologies, if the regulator considers so.

Conformity with P1-3 ECHR has been debated with respect to e-voting (see Courts' decisions in Germany, Austria, Estonia, Switzerland, France, among others).[9] Only recently have concerns about foreign interferences in elections led to closer scrutiny of the security of other digitally backed documents and solutions, namely registers, results transmission and calculation systems, etc. (e.g. in Germany and the Netherlands in 2017).

### *ii. Biometry*

Biometry introduces the possibility to capture and save in electronic format some physical characteristics (iris, fingerprint, face image, etc.) that should enable the unique identification of a person. It is introduced in elections in a hope to ensure among others the unique identification of voters and prevent multiple voting. 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 unique identification of voters. On election day, voters' physical, biometric characteristics are captured and compared to biometric information stored in

[9] For a worldwide comparative view, see Driza Maurer, Barrat (eds), *E-Voting Case Law – A Comparative Analysis*, Routledge 2015, 2017.

databases. Biometry in elections has been used in countries in South America or Africa. To a very few exceptions, Council of Europe countries do not consider biometry in elections. Issues of data protection and vote secrecy, as well as voter disenfranchisement due to errors in biometrical identification (false accept and false reject) are among the main reasons for not using biometry in elections in Europe so far. However, the 2018 Information report (French Senate, Ms Deromedi and Mr. Détraigne) on e-voting in France suggests considering unique identification of voters by introducing biometry.

Use of biometry in elections raises questions of compliance with P1-3 ECHR. How unique and permanent are biometrical characteristics to ensure the right to vote over time? Is it easy and fast to collect the biometrical information and authenticate the voter? Is the collection and use of such characteristics accepted by all voters? What about secure data storage to ensure secrecy and more generally what about system security?

### *iii. 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 decentralization, transparency and immutability.[10] The transactions being recorded across many computers, any involved record cannot be altered retroactively, without the alteration of all subsequent blocks.

A few experiences with blockchain voting have taken place at the local level.[11] Blockchain voting claims many advantages over traditional, centralized, paper-based voting systems. However, most properties (e.g. electronic identification, digital signatures to guarantee integrity of the data, strong cryptography, voter verifiability, multiple voting possibility) are not exclusive to blockchain and are present in "traditional" verifiable e-voting. Blockchain voting introduces at least one specific new feature: any information processed, via computing or data storage, is shared across multiple nodes (decentralisation). In a decentralized voting system, a set of entities must agree how a vote has been cast before recording it. This means that there is no single entity taking control: it is not only the organizer of the poll, the EMB, which validates a vote, but it could also be various accredited institutions (e.g. CoE, political parties, or local councils). This offers the advantage of protecting against internal threat: 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. As voters' identities are anonymized, the vote is allegedly secret. However, 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. (examples exist in Sweden or Geneva canton). One can envisage that administrations that embrace blockchain may be tempted to use it in the electoral cycle as well, e.g. to keep registers of voters, parties, etc. 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 will affect the whole cycle.

Blockchain raises a number of conformity questions with respect to P1-3 ECHR (the list is not exhaustive), namely on vote secrecy (data posted on the blockchain stays there), non-publication of intermediary results (the number of votes for each candidate is actually known before the voting is finished), but also on security, user-friendliness (important waiting times until a transaction or vote is concluded), respect of one-voter-one-vote principle (as computational power is important for decision-taking in this context), etc.

[10] Source Wikipedia, https://en.wikipedia.org/wiki/Blockchain

[11] E.g. the city of Zug in Switzerland conducted a mock blockchain vote on 25 June-1 July 2018. See the evaluation at http://www.stadtzug.ch/dl.php/de/5c00ff8dbd830/eVoting_Final_Report_ENG.pdf

### *iv. 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.[12] There are public as well as private clouds.

Organizations, 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 – so the common wisdom today – in-house IT expertise and solutions. Questions related to data protection, security of sensitive documents and processes and accountability are relevant here. The cloud may introduce new vulnerabilities (e.g. to security, secrecy and privacy, interoperability) and threats of attacks. At the same time forensics and investigation of irregularities become more complex. The use of cloud computing for documents and processes of the electoral cycle has not been specifically thematized so far.

Some questions specific to cloud computing relate to the secrecy and security of information stored on the cloud. Another one relates to interoperability and thus to the possibility to take back the data and maybe transfer it to another cloud.

### *v. Artificial intelligence*

Artificial intelligence (AI) refers to a wide range of methods, both current and speculative.[13] It refers to systems that display intelligent behaviour by analysing their environment and taking action – with some degree of autonomy – to achieve specific goals.[14] The AI field draws upon many fields. The traditional goals of AI research include reasoning and decision making (knowledge representation, planning, scheduling, search, optimization), learning (machine learning, neural networks, deep learning, decision trees etc.) and robotics (embodied AI; ability to move and interact with the physical world). So far, AI solutions are domain specific.

Main issues related to AI include data issues and explainability. AI systems need to process a lot of data to perform well and are as good as data that is fed to them. If the training data is biased (for instance not inclusive enough), so will be the AI trained on it and its decisions will be unfair. 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.[15]

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 even more sophisticated and difficult to predict than now “including more able to pursue highly customised objectives, and to adapt in real time”[16]. This should be taken very seriously by EMBs. At the same time, it is also expected that AI will be trained and used for cyberdefense.

AI may be envisaged in training and education, or in dispute resolution issues. It may be interesting for information retrieving purposes. However, greatest attention should be paid to the quality and other characteristics of the underlying data. It should also be underlined that the principle of open data does not

[12] Wikipedia, https://en.wikipedia.org/wiki/Cloud_computing

[13] European Parliamentary Research Service (2019) “How artificial intelligence works”, “Why artificial intelligence matters”. See also Wikipedia, https://en.wikipedia.org/wiki/Artificial_intelligence

[14] European Commission, indep. High-level expert group on artificial intelligence, “A definition of AI: Main capabilities and disciplines”, 8 April 2019

[15] 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

[16] UN High level panel Report, *The age of digital interdependence*, June 2019

apply to all kinds of data gathered in elections. Quite the opposite, detailed information on participation and on the content of the vote are covered by the secret suffrage requirement.

## b. Electoral cycle perspective

Below we consider the main phases of the electoral process, the new technologies used or envisaged and some questions of compliance with P1-3 ECHR.

### *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 these elements are initiated or drafted by the EMB, so it is also important for the EMB to have a structured and clear overview of all regulatory elements to be considered in the electoral cycle.

New technologies in this field would mainly help in preparing, organizing and retrieving information. Most importantly, legislation should regulate the use of new tech in the electoral cycle. It has proved difficult to write regulations that comply with higher-level principles, as decisions of the constitutional courts on e-voting in Germany and Austria have shown. It is unclear how the principles apply to new technologies. What should the regulation contain to be compliant? Concepts like legality or certainty of the electoral law are challenged by the complexity of new technologies and their rapid evolution.

One issue are the concepts used. In an analogic world, security and controls, for instance, are considered in a static way, as products, whereas in a high-tech context, security and controls must evolve daily, to respond to evolving vulnerabilities and threats and thus to new risks.  Some compare this to an arms' race. This is/should be reflected in regulation. In the analogic world, EMBs must ensure security except in exceptional cases such as *force majeure*. How to define their role in a digitized context? It is easy to accept *force majeure* in low tech contexts. Is hazard in software acceptable (with reference to AI)? As new tech evolves through trial and error, what should an EMB ensure? What positive obligations arise from its task of ensuring conformity with P1-3 ECHR in the electoral cycle?

The answers are far from trivial. Constitutional courts (e.g. Germany, Austria), parliament, government and watchdog organisations (e.g. Netherlands, Norway, France) have recognized the shortcomings of existing regulations for instance on e-voting. Such regulations, inherited from the '70, 80' and 90'ties, should evolve to take account of newest technologies. In a few cases only (e.g. Belgium, Estonia, Switzerland) the regulator has introduced upgraded regulations. Their suitability is tested in practice and it appears that such regulations need to continue to evolve (see e.g. the Swiss 2019 transparency exercise in i-voting and lessons learned on verifiability, transparency and certification).[17] Guidance from CoE has been crucial in inspiring countries to update regulations on e-voting. However, a most recent wave of questions has not yet been discussed, including the following: how to check and control the verifying mechanisms? How to evaluate trust assumptions which are necessary in verifiable e-voting? How to parameter transparency (what happens after source code is published), etc.? A forum offering ongoing discussion and exchanges is necessary as we learn by doing.

E-voting is the most advanced field also with respect to regulation of new technology. Other high-tech solutions used in the electoral cycle are regulated, at best, from a narrow IT management perspective, or are not regulated at all. Their conformity with P1-3 ECHR and national electoral principles has, so far, not been

[17] 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

questioned. Attempts by EMBs to upgrade such regulations meet sometime with resistance.[18] However, things are changing quickly since 2016 and the thematization of foreign countries meddling in elections by "hacking" e-backed electoral cycle solutions. Recent examples from the 2017 elections in the Netherlands (counting and tabulation software) and Germany (results transmission software) show that processes vital for the outcome of the election face similar challenges to e-voting and should be better regulated. This offers an opportunity to CoE to continue to provide guidance, based on work done in the e-voting field, which is allegedly the most complex use of new tech in elections.

In addition to providing guidance on the implementation of universal, equal, free and secret elections, Rec. (2017)5 also deals with some important conditions such as gradual introduction of new technologies, accountability (certification, audits), distribution of responsibilities between state authorities, the private sector and the electorate, transparency and observation, reliability and security, handling of sensitive data, data standards and interoperability. These questions are relevant to all digitization.

The replies to the questionnaire show that guidance from CoE on implementing the principles of democratic elections and referendums to e-voting (Rec (2017)5) is considered important by countries with e-casting of the vote systems (such as Belgium, Estonia and Switzerland), countries with only e-counting (such as the Czech Republic, Denmark or Hungary) and others that consider such solutions.

The replies also show that further discussion at the regional level is needed especially on issues such as cybersecurity, verification of the vote, digital identity, contingency procedures in case of interruption of communication, etc. which should receive more attention also at the legislative level. This, also with a view to the next wave of changes in e-voting regulation envisaged (e.g. in Estonia in 2021 and Switzerland, from 2020). Whereas Rec(2017)5 is meant to be stable, the guidelines need to evolve.

### *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 back-up solutions are foreseen.

### *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, 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, regulates opinion polls.

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

### *iv. Registration*

As mentioned under digitization, 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 all digitized probably in all CoE countries.

[18] 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.

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 P1-3, one issue faced by all registers is the unique identification of individuals, i.e. of voters and candidates. The unique identification serves the purpose of ensuring equal suffrage (one person one vote) as well as respect of electoral rules on candidacy. In analog, 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 for example of quick verification and effective prevention of multiple voting or multiple candidacy. In addition to biometrics (discussed above), another discussed solution is the unique e-identification. It is not widespread. Estonia uses e-IDs for voter authentication. In other countries attempts have been made to use alternative unique identifiers, such as social security numbers, for instance for identifying candidates. So far, this has been fiercely resisted, mainly by data protection watchdogs. Data protection has prevailed over respect for other principles (candidacy rules or one-person-one vote). Lately, there is a trend for data protection watchdogs to be more open to such use and also a trend towards broader use of e-IDs in general as such unique identification will allegedly facilitate transactions in all areas of life.

### *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 report.

### *vi. Voting operations*

This phase refers to the election process, from opening to closing of the vote and subsequent counting, verifying and publishing of results. Parts of this process can be supported by digital solutions, including e-identification of voters, e-voting, e-counting, e-transmission of results, where such solutions are used, which were mentioned under technology perspective/digitization. CoE has done pioneering work in the e-voting and e-counting areas (see Rec(2017)5 and associated guidelines). Guidance on the use of new technologies for other voting operations is discussed by this report (see also chap. 4 below).

### *vii. Election results*

In addition to collecting, tabulating and publishing results, EMBs use new-technology-based solutions also to conduct audits and verifications to check the correctness of results. As mentioned, there exist statistical methods to check the plausibility of results, i.e. to identify electoral irregularities by statistical methods.[19] Statistical methods evaluate probabilities of correctness of results based on data from previous elections. That implies that they need to be "fed" with digitized data from current and previous elections. As for AI, the quality and quantity of data are crucial for these methods to function optimally.

EMBs may be dispute resolution authority. New tech solutions may be used to retrieve information. There is not yet talk of predictive justice here. However, tools used to retrieve information are of interest to help EMBs take quick and correct decisions. Arguably, such tools will help voters to better understand their rights. They can as well improve access to justice for complaining users (voters, parties, etc.).

### *viii. Post-election duties*

Such duties include deletion or archiving of 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. Same remarks as for planning apply here.

[19] 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 of issues related to new technologies and their use in the different phases of the electoral cycle shows that the most widespread and necessary one is digitization, which is also the founding layer of any other new technology, including biometry, blockchain, cloud computing and artificial intelligence.

Digitization raises questions of implementation of and compliance with the principles and conditions for democratic elections (P1-3 ECHR and Venice Commission’s Code of good practice in electoral matters and Code of good practice in referenda). These questions have been dealt in quite some depth with respect to e-voting, but not with respect to other elements of the electoral cycle. Recent developments show that such aspects too need regulation. Requirements for sensitive documents and processes may be aligned with requirements for e-voting. Also, it is felt that more work, including at the regional level, is needed on issues like cybersecurity in elections, verification of the vote, digital identity, contingency procedures in case of interruption of communications, etc.

The overview also shows that some issues are transversal, i.e. of interest to all digital technologies and all phases of the electoral cycle. These include cybersecurity, data protection and the roles and responsibilities of the actors involved. Some of them are dealt by existing instruments of CoE not specific to elections. However, elections remain a case apart, to which stronger requirements apply. CoE may envisage consolidating and deepening election specific guidance in these areas.

Data protection

The CoE instrument is Convention 108+ for the protection of individuals with regard to the automatic processing of personal data, which takes account of several other existing international instruments. At the EU level, the main instrument is the Regulation (EU) 2016/679 General Data Protection Regulation (GDPR). CoE 108+ and GDPR were developed in parallel and are consistent with each other. GDPR amplifies some principles of Convention 108+.

However, some data used in elections are qualified data. Their processing should only be allowed if appropriate safeguards are enshrined in law (art. 6 Convention 108+). Specific requirements apply, which should be stronger than those of Convention 108+ and GDPR. However, in many cases, it is not clear for those in charge, what are the requirements. This shows that these are relatively new preoccupations to EMBs. And they are complex, given the interplay between different instruments and the specificities of elections. By clarifying how main categories of data used in elections should be handled, the new CoE guiding document would fill this lacuna. CoE standards should offer combined expertise. For instance, use of cryptography is an important measure to protect some of these data.

Cybersecurity

Cybersecurity is a relatively recent but hot topic for EMBs. Regulations dealing with cybersecurity of critical infrastructure are being introduced at the national level. There is also a trend to declare elections critical infrastructure (USA, European Union, etc.). EMBs must ensure that electoral principles and rules are respected when introducing and enforcing cybersecurity measures.

The same approach as for data protection can be adopted for security of new technology solutions used in elections. Again, this is transversal. It requires EMBs to think about solutions’ security, hardware security and how their corruption, interruption, etc. could affect the ongoing election. Back-up measures are foreseen. Examples of cities/administrations whose administrative processes were blocked due to ransomware (e.g. Baltimore in May 2018) show what could go wrong and how critical processes could become the target of politically, financially etc. motivated hackers.

Guidance by CoE would help to align national general legislation on cybersecurity and critical infrastructure with specificities of the election field.

Public-private cooperation

Public-private cooperation is an important aspect of the use of new technologies in elections. Introduction of new technology solutions as well as their control are done mostly by the private sector. When introducing e-voting for instance, the EMB should make sure that procurement conditions include requirements that are important for the P1-3 ECHR compliance of systems and solutions.

One important aspect is clarification of responsibilities. Political responsibility should lie with the EMB. But what happens in case of proved errors? Who bears responsibility? This needs to be clarified before starting the cooperation.[20]

## 4. WORK AT CDDG GT-DT

What are the implications of the issues discussed above on the standard-setting work at CDDG and GT-DT?

### a. CoE guidance on P1-3 ECHR compliant use of new technology throughout the electoral cycle

The existence of digital technology and its application to nearly all aspects of life including elections, is a fact which cannot be put into question.[21]

New technologies used in elections should comply with P1-3 is the ECHR (and other principles not discussed here). Venice Commission has identified the elements of the European electoral heritage, i.e. the requirements derived from P1-3 ECHR which are common to the region. As already done in the e-voting field (see Rec (2017)5), CoE may introduce standards which offer guidance on P1-3ECHR compliant use of new technologies used throughout the electoral cycle.

As mentioned, CoE is the only regional organisation with the mandate to establish principles and standards for elections. Furthermore, it has already done so in the e-voting field which is recognized and appreciated by countries and organisations worldwide.

In order to identify countries' practices and good practices, issues and questions, areas where guidance is most appreciated, the kind of guidance needed, etc., it may be necessary submitting EMBs and other interested entities a detailed questionnaire. EMBs are the central authorities in charge of these issues at the national level. Other interested stakeholders include academia, namely experts who are already active in elections and digital technology, solution providers, data protection watchdogs, NGOs representing citizen's interests at large, etc. A broad consultation would contribute to the quality and acceptance of standard-setting and later of standards.

[20] A recent example is that of the transparency exercise that took place in Switzerland at the beginning of 2019: as assurances offered by the provider and by the certification authority proved to be in part erroneous, e-voting was not conducted at the Mai vote and October election (see fn. 17). Some cantons said they intended to sue the provider.

[21] European Commission for Democracy through Law (Venice Commission) *et al.*, 2019, "Draft Joint Report on Digital Technologies and Elections"

## b. Content of guidance

Given the broad spectrum of the electoral cycle and of the new technologies to be covered, in addition to expert advice, it is necessary to collect countries experiences, questions and expectations through a new detailed questionnaire, as proposed above.

It is however almost certain that guidance will be general and broad. So, in addition, there will be need for expertise focused on specific questions that will arise in different countries, as use of new technologies in elections becomes a permanent topic. Consideration could be given to creating a pool of expertise that deals with new technologies in elections at the Centre of competence of CDDG so as to ensure, also at a more practical and detailed level, compliance of practical implementations with the future CoE standard on new technologies in elections and P1-3ECHR.

The replies to the 2019 questionnaire offer a few hints as to the content of the future standard. Namely, some issues should be dealt at the regulatory level, including cybersecurity in elections, verification of the vote, digital identity, contingency procedures. Countries have expressed the wish and need to know more about best practices related to e-enabled processes in the electoral cycle. Finally, countries have also underlined the necessary coordination with activities of other bodies and activities at CoE, namely Venice Commission, CoE electoral assistance, cybersecurity or data protection.[22]

Through its work in standard-setting and possibly in offering focused expertise to countries' specific questions, CoE may help in building capacities at the national EMB level on regulation and use of new technologies in elections that is compliant with conventional principles. Such help is aimed at maximising benefits and minimizing harms that come with such new technologies so that their use in elections lies on a foundation of respect for free elections and other human rights.

[22] For instance, important relevant work is done by the Cybercrime Convention Committee (Budapest Convention) namely on issues of interstate cooperation to counter cybercrime.

## 5. 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,* of 26 June 2019

Council of Europe, *Convention 108+, Convention for the protection of individuals with regard to the 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 no. 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*, of 13 February 2019

Council of Europe, *Recommendation of the Committee of Ministers to member States on standards for e-voting, 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.*, *Draft Joint Report on Digital Technologies and Elections,* 7 June 2019

IDEA, *Cybersecurity in elections. Models of interagency cooperation*, 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