Strasbourg, 20 November 2019

CDDG(2019)7
Item 7.2 of the agenda

EUROPEAN COMMITTEE ON DEMOCRACY AND GOVERNANCE (CDDG)

NEW TECHNOLOGIES IN THE ELECTORAL CYCLE. GUIDANCE FROM THE COUNCIL OF EUROPE?

Ardita Driza Maurer
Jurist, independent consultant, Switzerland
September 2019

For information

Expert report
prepared for the
Directorate General of Democracy
Democratic Governance Department

Content

DEFINITIONS AND APPROACH

Electoral cycle

From the perspective of the Election Management Body (EMB), an electoral cycle encompasses all steps and processes that fall within the extent of functions, responsibilities and powers of the EMB 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 elements of elections' cycle are the design and drafting of legislation, the recruitment and training of electoral staff, electoral planning, voter registration, the registration of political parties, the nomination of parties and candidates, the electoral campaign, polling, counting, tabulating and publishing results, the resolution of electoral disputes, reporting, auditing and archiving.

The conduct of direct democracy votes involves similar steps and additional ones, like the formal and/or material approval of the (initiative or referendum) proposal, control of the form for gathering signatures of supporters, reception and control of validity of signatures, counting, validation and publication of results and eventually organisation of the vote if the collection was successful in gathering the required number of valid signatures. Then, like in elections, the EMB informs voters, plans and conducts the vote.[1]

In this document, the term election/electoral cycle refers to both elections and direct democracy votes.

New technologies

Digital technology evolves rapidly. "New technologies" refer to the most recently introduced ones in the electoral cycle. Yesterday, it was the digitization of documents/procedures and biometry. Today, "new" often implies blockchain, cloud computing, internet of things or artificial intelligence.

Method

New technologies used in the electoral cycle should comply with the right to free elections (P1-3 ECHR) as well as other rights such as freedom of expression, non-discrimination, etc. We focus here on P1-3 ECHR. As the guardian of the values enshrined in the ECHR and its protocols, the Council of Europe (CoE)'s core mission is to oversee the implementation of ECHR in and by countries in the region. This is so also for election related activities.

Pursuant to P1-3 ECHR and case law of the ECtHR, the EMB (i.e. the State) has the positive obligation to make sure that all activities in an electoral cycle, including e-backed ones, comply with the right to free elections.

[1] IDEA, Electoral Management Design, 2014: 12; 16; 75-77

It's clear that new technologies improve and facilitate several aspects of elections. However, rapid change, complexity and limited understanding (especially multidisciplinary one), unpredictability and even attacks against electoral processes – which came with new technologies – do fragilize the EMBs. These are furthermore under social and political pressure to modernise while also guaranteeing overall security.

The question: do we need guidance from CoE on use of new technologies in elections, is to be read against this background. To assess this question in a concise manner, we proceed as follows. We first review the characteristics, uses and issues of some new technologies. Then we look at the different phases of the electoral cycle to find out what new technologies/solutions are used or envisaged and what are or could be the conformity issues. Finally, we propose some scenarios for CoE to provide guidance and envisage what happens if it decides not to work on further guidance.

Protection of elections from manipulations of the opinions (fake news, [Facebook] algorithms, etc.) is not discussed here as it is subject of work in other forums, at the Council of Europe and other organisations.[2]

QUESTIONING THE USE OF NEW TECHNOLOGIES

Technology perspective

Digitization

Digitization is the conversion of text, pictures, or sound into a digital form that can be processed by a computer. It is the founding layer of all new technology. Its main advantage is to allow for computer treatment of digitized information: error free, efficient, quick, etc.

In the CoE region, most documents used in the electoral cycle are digitized. Examples include registers and databases of information. Digitization of processes is more challenging, especially when they are conducted over the internet. E-registering, e-identification of voters (e-pollbook), e-voting (both on voting machines in polling stations and over internet), e-counting, e-transmission of results (from polling stations to a central unit for instance) are examples of digitized electoral processes.

[2] See e.g. Venice Commission, Draft joint report of the Venice Commission and of the directorate of information society and action against crime of the directorate general of human rights and rule of law of 7 June 2019, CDL(2019)002.

One dilemma is deciding how should a digitized process look like: should it mimic the "traditional" way of doing (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 instance, from an "equal suffrage" perspective, an e-voting channel is not allowed to offer more/different possibilities to voters than a traditional channel. However, another logic, centred on principles and not processes, has also been employed. It focuses on principles who need to be protected. For instance, e-voting being exposed to specific risks, to ensure respect for the principle of "free and secret suffrage", verifiability is introduced. Verifiability enables the voter to verify her own vote as well as the general result which is a new, disruptive process.

Biometry

Biometry introduces the possibility to capture and save in electronic format some physical characteristics (iris, fingerprint, face image, etc.) that enable the unique identification of a person. It has been introduced in a hope to ensure among others the unique identification of voters and prevent multiple voting, especially in countries with less/no strong traditional registers.

Biometry in elections (unique identification of voters by capturing physical, biometric characteristics and comparing them to information stored in databases) is mainly used elsewhere than in Europe (South America, Africa, etc.). Voter secrecy, voter disenfranchisement and data protection are among the main concerns and reasons for not accepting biometric registration of voters in Europe.

Blockchain

A blockchain is, an immutable time-stamped series record of data that is distributed and managed by a cluster of computers. Blockchain's main characteristics are decentralization, transparency and immutability.[3] 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.[4] Blockchain voting claims many advantages over traditional, centralized, paper-based voting systems. However, most properties (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 and disruptive 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

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

[4] 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

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 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.

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.[5] 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.

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

Artificial intelligence

Artificial intelligence (AI) refers to a wide range of methods, both current and speculative.[6] It refers to systems that display intelligent behaviour by analysing their environment and taking action – with some degree of autonomy – to achieve specific goals.[7] 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; general intelligence is among the long-term goals.

There is currently no use of AI in the electoral cycle to our knowledge. Relying on a (possible) future general AI for better decision-taking, would virtually mean the end of democracy as we know it today. However, AI techniques are increasingly used in other fields, including justice. So called virtual tribunals or predictive justice (e.g. in Canada) are systems used to advise judges.

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.[8]

AI may have an impact on new tech 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"[9]. 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.

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

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

[8] 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

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

Electoral cycle perspective

Legislation

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 them to have a structured and clear overview of all regulatory elements to the extent that they need to be considered in the electoral cycle.

The use of new tech in this field is mainly to prepare, organize and retrieve information. But, 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. This is even more so as it is still unclear how the principles apply to new technologies. What should regulation contain to be compliant? How to handle legality or certainty of the law given the complexity and rapid, industry driven changes in new tech? How to control conformity? Etc.

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 (e.g. Swiss 2019 transparency exercise and lessons learned on verifiability, transparency and certification). Guidance from CoE has been crucial in inspiring countries to update regulations. However, the newest wave of questions has not yet been discussed at the CoE CAHVE, 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.

And e-voting is the most advanced field, with respect to regulation of new technology. Most other high-tech solutions used in the electoral cycle are still 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 questioned. Attempts by EMBs to upgrade such regulations have been largely resisted (see discussion on regulation of e-counting solutions in Switzerland and resistance from cantons). 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 challenges similar to e-voting and should be better regulated. There is now consensus that better regulation is needed. This presents a big opportunity for 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.

Planning and financing

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 the back-up solutions offered.

Education, information, regulation of conduct

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.

Registration

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. When the electoral register is based on registration, the authority in charge must determine if the voter is eligible to vote. 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.

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 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 verifying quickly and effectively preventing multiple voting or multiple candidacy. In addition to biometrics (discussed above), another discussed solution is the unique e-identification. It is not widespread. In some cases attempts have been made to introduce alternative unique identifiers, usually a social security number. So far, both the introduction of e-IDs and the use of other unique identifiers like social security numbers, in the election cycle, has been fiercely resisted, mainly by data protection watchdogs. Data protection has so far prevailed over respect for other principles and rules derived from P1-3. 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 as such unique identification allegedly will facilitate transactions in all areas of life. This increases the importance of protection of data used in elections.

Voting, counting, verifying and publishing results

This phase refers to the election process, from opening to closing of the vote and subsequent counting, verifying and publishing of results. Part of this process are e-identification of voters, e-voting, e-counting, e-transmission of results, where such solutions are used. CoE has done pioneering work in the e-voting and e-counting areas (see Rec(2017)5 and associated guidelines).

Even in countries without e-voting, EMBs use software to plan and conduct related tasks. One example are audits and verifications to check the correctness of results. There exist statistical methods to check the plausibility of results (Venice Commission has also studied this aspect). As for AI, statistical methods need to be "fed" with digitized data from current and previous elections. Based on such data, they draw conclusions on the correctness of results. Again, the quality and quantity of data are crucial for these methods to function optimally.

Dispute resolution

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 make correct and quick 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.).

Post-election duties

Such duties include 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.

Transversal issues perspective

Some transversal issues like data protection or security of IT systems and information are dealt by existing instruments. However, elections remain a case apart, to which specific (stronger) requirements apply which should be listed in the specific regulation.

Data protection

The general instrument in the region is Convention 108+ for the protection of individuals with regard to the 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). Their provisions address unlawful use of personal data also in an electoral context. CoE 108+ and GDPR were developed in parallel and are consistent with each other. GDPR amplifies some principles of Convention 108+

However, data used in elections or linked to political opinion are a special category of sensitive data. Their processing should only be allowed if appropriate safeguards are enshrined in law (art. 6 Convention 108+). In writing such laws, EMBs and the legislator in general, need to have combined expertise. For instance, use of cryptography is an important measure to protect some of these data. Guidance may be useful here.

(Cyber)security

Cyber security is a relatively recent topic of 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 (cf. the US or Sweden; also the EU initiatives related to the 2019 EU parliament elections go in the same direction). EMBs must ensure that electoral principles and rules are respected when introducing and enforcing cybersecurity measures.

Public-private cooperation

Public-private cooperation is an important aspect of the use of new technologies in elections. Namely new tech solutions as well as control of these solutions 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 cooperation. A recent example is that of the transparency exercise that took place in Switzerland at the beginning of this year: 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. Some cantons said they intended to sue the provider[10].

[10] 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

RECOMMENDATIONS

Based on the identified uses and possible future use of new technologies in elections, the following four scenarios envisage possible future guidance from CoE.

Scenario 1: Multidisciplinary discussion framework

Increasing dependence on new technology

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 (Venice Commission 2019).

Furthermore, there is a trend to introduce ever newer technologies to solve old problems (e.g blockchain to ensure that documents like registers or votes cannot be modified) or to solve problems that came with the new technologies already in use (e.g. AI trained algorithms to protect from cyber threats).

Currently there is a patchwork of documents and solutions and a patchwork of approaches on using new technologies in the electoral cycle, within member states and across the region. This "organic" development has offered valuable insight. However, to the risk of losing oversight and control, it is necessary to review and consolidate their regulation, to strengthen their compliance with P1-3 ECHR and make the electoral cycle fit to face today's risks (and hopefully exploit opportunities) that come with new tech.

As new technologies become a permanent topic, EMBs need a structured, multidisciplinary discussion framework to address the issues that come with new technologies.

The discussion takes place at the national level, where the responsibilities for organising elections lie. Yet, EMBs do not usually have the multidisciplinary expertise, human, financial and time resources to thoroughly address the issue on their own. Even if they did, it is highly desirable to coordinate solutions at a larger scale.

Guidance from CoE on e-voting – the most complex aspect of the electoral cycle – could naturally extend to cover use of new technologies throughout the electoral cycle. CoE's mission makes it the appropriate organisation to offer technical and practical guidance to member States on how to ensure, at the regulatory level, that use of new technologies complies with P1-3 ECHR.

Human-rights centred

"*Shared values become even more important during periods of rapid change, limited information and unpredictability… It would be useful for the private sector, communities and governments to conduct digital cooperation initiatives by explicitly defining the values and principles that guide them*".[11]

[11] UN HLP Report (2019:30)

CoE's mission to ensure respect of ECHR extends to elections and respect of P1-3 ECHR as well. In today's context this means providing guidance on how the principles of free elections are implemented / complied with when using new technologies. CoE has already a lot of experience with ensuring respect for free elections in the e-voting context (see the 2004 and 2017 Recommendations on e-voting). (E-)voting being the most complex process of the electoral cycle, CoE has an important expertise in defining the meaning of principles in an e-voting context and operationalising the principles through more detailed guidelines. This existing expertise could extend to the whole cycle. Human – rights should be enforced by design. So the discussion on compliance should start right from the beginning of the elaboration of solutions based on new tech.

Through such guidance, CoE helps build human and institutional capacity at the EMB level on using new technology that complies with principles, in synergy with other work on elections at CoE (e.g. ElecData), with the aim of increasing transparency of regulations, cross-evaluation and harmonisation. It offers a "help and information desk" to governments and others to understand digital issues in the context of elections and respect for principles to maximise benefits and minimize harms. It helps ensure that digital solutions are built on a foundation of respect for free elections and other human rights.

Holistic and multidisciplinary

As a convener, CoE provides a unique space not only for debating principles but also for multidisciplinary discussion, and this at the regional level. In e-voting as well as in many other fields, there is growing consensus that we need a "system" approach. As solutions are interconnected, so are risks and opportunities. Cooperation and regulation should be multistakeholder and adaptive. This calls for a dedicated platform/forum for discussing these issues. This is increasingly necessary given the complexity of new solutions, like AI. A dedicated forum responds to the desire and need for more tangible outcomes, more active participation by governments and the private sector, more inclusive processes and better follow-up.

Scenario 2: Guidance on aspects of data protection

Work in this area would focus on protection of data that feed in new technology solutions. The question here is what does respect for the principles (right to free elections), particularly the secret suffrage, entail? As seen above, data used in elections is qualified data. 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 requirements apply. This shows that these are relatively new preoccupations to EMBs. And they are complex, given the interplay between different existing instruments and specificities of elections. By clarifying how main categories of data used in elections should be handled, the new guiding document would fill this lacuna.

By adopting a transversal approach, EMBs are required to adopt a holistic approach and consider all data they possess. This will arguably improve data protection.

Scenario 3: Guidance on aspects of security

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.

By providing guidance CoE would help align national general legislation on cyber security and critical infrastructure with specificities of the election field.

Scenarios 1, 2 and 3 are complementary. Guidance on data protection or security in elections, to remain pertinent, needs to be reviewed on a continued basis, hence the necessity of a discussion forum.

Scenario 4: No new guidance

What if no new guidance is issued? Presumably CoE will continue to work on e-voting as foreseen in Rec(2017)5. Most issues can be discussed there, provided the discussion forum (periodic meetings) is activated. However, the discussion will remain focused on e-voting and will ignore specificities of other elements of the cycle.

Other stakeholders, mainly providers and other international organisations will continue to work on the topic and occupy the ground.[12] Despite their merits, no other organisation has the mandate of CoE and the possibility to issue guidance on how to regulate use of new tech in elections.

Other bodies inside CoE will continue to work on election-related aspects. A very good example is the work of the committee of the Budapest Convention. However, these will remain scattered efforts (as opposed to systemic, holistic) because, for instance, Budapest Convention only deals with one (important) aspect of cybersecurity which is interstate cooperation in reacting in case of breaches.

[12] Just recently UNESCO/UNDP started work on a publication "Elections and Internet, Social Messaging and AI – Guide for Electoral Practitioners". Another example is the UN "Global Commission on Stability in the Cyberspace" which is developing proposals, among others, for non-interference in elections and agreement not to attack critical infrastructure (UN HLP Report 2019: 27)

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+, Modernised 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