Strasbourg, 1 September 2020

CDL-EL(2020)005

Engl. only

EUROPEAN COMMISSION FOR DEMOCRACY THROUGH LAW

(VENICE COMMISSION)

Collection of reports

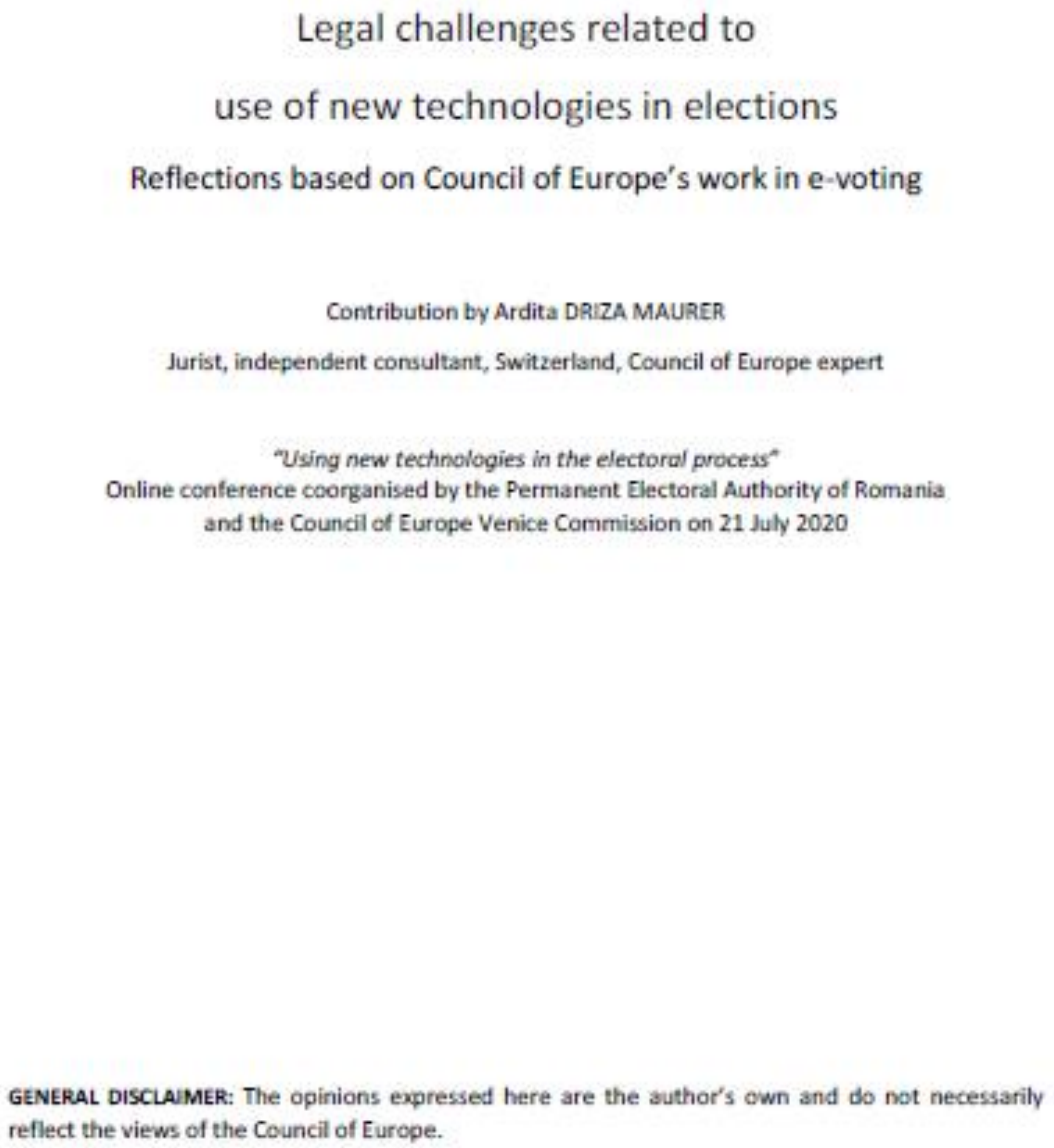
USING NEW TECHNOLOGIES IN ELECTORAL PROCESS

An online meeting held on 21 July 2020

This document will not be distributed at the meeting. Please bring this copy.
www.venice.coe.int

Contents

Report by Ms A. Driza Maurer



Legal challenges related to use of new technologies in elections

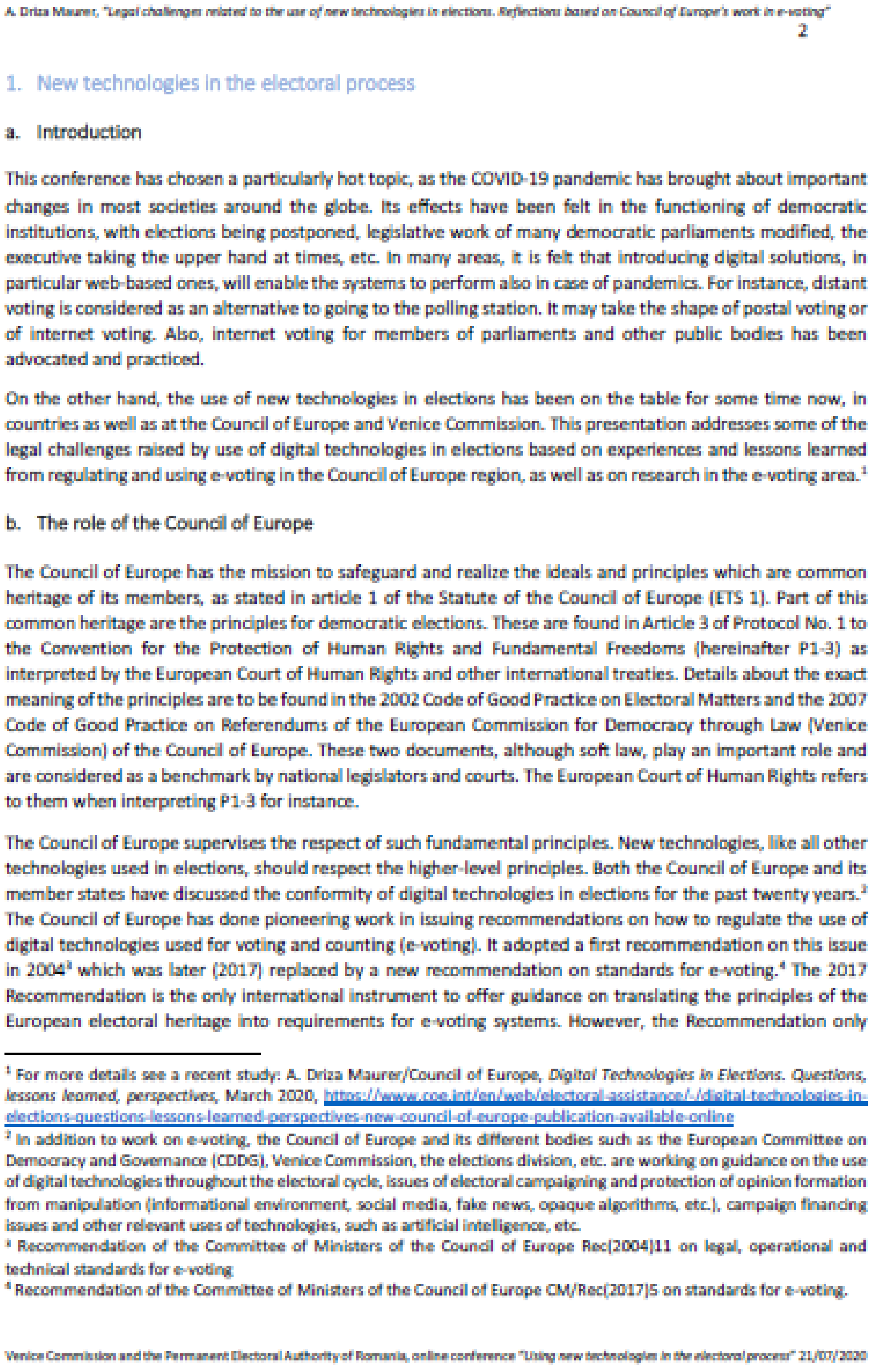
Reflections based on Council of Europe's work in e-voting

Contribution by Ardita DRIZA MAURER

Jurist, independent consultant, Switzerland, Council of Europe expert

"Using new technologies in the electoral process"
Online conference coorganised by the Permanent Electoral Authority of Romania
and the Council of Europe Venice Commission on 21 July 2020

GENERAL DISCLAIMER: The opinions expressed here are the author's own and do not necessarily reflect the views of the Council of Europe.



1. New technologies in the electoral process

a. Introduction

This conference has chosen a particularly hot topic, as the COVID-19 pandemic has brought about important changes in most societies around the globe. Its effects have been felt in the functioning of democratic institutions, with elections being postponed, legislative work of many democratic parliaments modified, the executive taking the upper hand at times, etc. In many areas, it is felt that introducing digital solutions, in particular web-based ones, will enable the systems to perform also in case of pandemics. For instance, distant voting is considered as an alternative to going to the polling station. It may take the shape of postal voting or of internet voting. Also, internet voting for members of parliaments and other public bodies has been advocated and practiced.

On the other hand, the use of new technologies in elections has been on the table for some time now, in countries as well as at the Council of Europe and Venice Commission. This presentation addresses some of the legal challenges raised by use of digital technologies in elections based on experiences and lessons learned from regulating and using e-voting in the Council of Europe region, as well as on research in the e-voting area.[1]

b. The role of the Council of Europe

The Council of Europe has the mission to safeguard and realize the ideals and principles which are common heritage of its members, as stated in article 1 of the Statute of the Council of Europe (ETS 1). Part of this common heritage are the principles for democratic elections. These are found in Article 3 of Protocol No. 1 to the Convention for the Protection of Human Rights and Fundamental Freedoms (hereinafter P1-3) as interpreted by the European Court of Human Rights and other international treaties. Details about the exact meaning of the principles are to be found in the 2002 Code of Good Practice on Electoral Matters and the 2007 Code of Good Practice on Referendums of the European Commission for Democracy through Law (Venice Commission) of the Council of Europe. These two documents, although soft law, play an important role and are considered as a benchmark by national legislators and courts. The European Court of Human Rights refers to them when interpreting P1-3 for instance.

The Council of Europe supervises the respect of such fundamental principles. New technologies, like all other technologies used in elections, should respect the higher-level principles. Both the Council of Europe and its member states have discussed the conformity of digital technologies in elections for the past twenty years.[2] The Council of Europe has done pioneering work in issuing recommendations on how to regulate the use of digital technologies used for voting and counting (e-voting). It adopted a first recommendation on this issue in 2004[3] which was later (2017) replaced by a new recommendation on standards for e-voting.[4] The 2017 Recommendation is the only international instrument to offer guidance on translating the principles of the European electoral heritage into requirements for e-voting systems. However, the Recommendation only

[1] For more details see a recent study: A. Driza Maurer/Council of Europe, *Digital Technologies in Elections. Questions, lessons learned, perspectives*, March 2020, https://www.coe.int/en/web/electoral-assistance/-/digital-technologies-in-elections-questions-lessons-learned-perspectives-new-council-of-europe-publication-available-online

[2] In addition to work on e-voting, the Council of Europe and its different bodies such as the European Committee on Democracy and Governance (CDDG), Venice Commission, the elections division, etc. are working on guidance on the use of digital technologies throughout the electoral cycle, issues of electoral campaigning and protection of opinion formation from manipulation (informational environment, social media, fake news, opaque algorithms, etc.), campaign financing issues and other relevant uses of technologies, such as artificial intelligence, etc.

[3] Recommendation of the Committee of Ministers of the Council of Europe Rec(2004)11 on legal, operational and technical standards for e-voting

[4] Recommendation of the Committee of Ministers of the Council of Europe CM/Rec(2017)5 on standards for e-voting.

deals with e-voting. Other digital solutions used during the electoral cycle, independently from any e-voting, are not covered by the Recommendation, formally speaking, as they do not correspond to the definition of e-voting. Such solutions, developed independently from e-voting, may be e-registers, vote tabulation and results transmission systems, solutions for voter information, etc. However, to the extent that they use similar technologies, are bound by the same high-level principles, are subject to similar threats and play a role in the integrity of elections, some analogies can be drawn between e-voting and other digital solutions used in elections.

Apart from e-voting, the Council of Europe has examined also other aspects of use of digital technologies in elections.[5]

c. International legal standards

Elections, and technologies used in elections, should respect several principles and conditions that lend them the democratic status. We focus on free elections, i.e. the principles of universal, equal, free, secret and direct suffrage and the conditions for implementing these principles, such as procedural guarantees of impartiality, transparency and observation.[6] Other rights such as freedom of expression, non-discrimination, freedom of movement, etc. should also be complied with. However, ensuring compliance with free elections is the most challenging part. We focus on that.

The higher-level principles are to be found in international instruments and national ones, typically the constitution. Our focus here is on international legal standards, which are shared by all countries. However, countries' legislations also include country specific legal principles which should be considered. They apply throughout the electoral cycle, also to new digital technologies. Complying with international standards can be seen as a starting point, a minimum. Given that digital solutions will be used in a specific electoral cycle, compliance with international standards is not enough. Solutions should also comply with national specific requirements.

The principle of free elections is foreseen in binding international instruments: article 21 of the 1948 United Nations Universal Declaration of Human Rights (UDHR),[7] article 25 of the 1966 UN International Covenant on Civil and Political Rights (hereinafter – ICCPR) and article 3 of the additional (first) Protocol to ECHR (hereinafter P1-3 ECHR). Authoritative interpretations (e.g. ICCPR's General Comment 25), the case law of ECtHR namely on P1-3, political commitments such as the 1990 Copenhagen Document of the Conference for Security and Co-operation in Europe (CSCE) interpret and complete the list of elements of free elections. The Charter of Fundamental Rights of the European Union contains similar rights and applies to EU countries. Pursuant to P1-3 ECHR[8] and case law of the ECtHR, the State has the positive obligation to make sure that all activities led by it within an electoral cycle, including those backed by new technologies, comply with the mentioned principles.

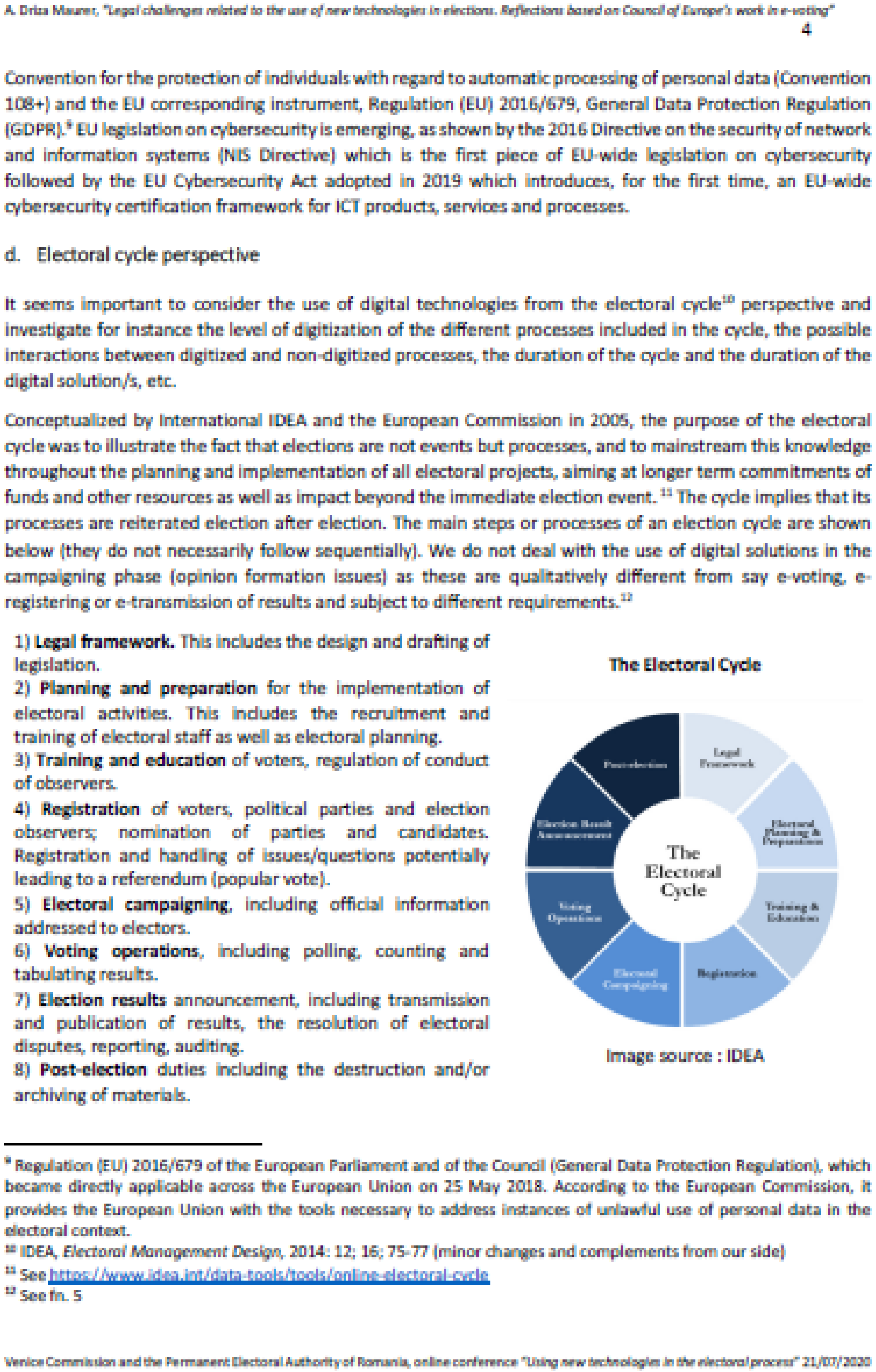
As we discuss the use of *digital technologies* in elections, other international legal standards are relevant: the Convention on Cybercrime of the Council of Europe (Budapest Convention), the Council of Europe Modernised

[5] 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.

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

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

[8] 45 out of 47 member states have ratified this protocol. Switzerland and Monaco have signed it but not yet ratified. However, to the exception of the accepted lack of secrecy in (only) some local elections where voting by raising hands is used, electoral principles of Swiss law are usually considered to be stricter compared to P1-3 ECHR.



Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108+) and the EU corresponding instrument, Regulation (EU) 2016/679, General Data Protection Regulation (GDPR).[9] EU legislation on cybersecurity is emerging, as shown by the 2016 Directive on the security of network and information systems (NIS Directive) which is the first piece of EU-wide legislation on cybersecurity followed by the EU Cybersecurity Act adopted in 2019 which introduces, for the first time, an EU-wide cybersecurity certification framework for ICT products, services and processes.

d. Electoral cycle perspective

It seems important to consider the use of digital technologies from the electoral cycle[10] perspective and investigate for instance the level of digitization of the different processes included in the cycle, the possible interactions between digitized and non-digitized processes, the duration of the cycle and the duration of the digital solution/s, etc.

Conceptualized by International IDEA and the European Commission in 2005, the purpose of the electoral cycle was to illustrate the fact that elections are not events but processes, and to mainstream this knowledge throughout the planning and implementation of all electoral projects, aiming at longer term commitments of funds and other resources as well as impact beyond the immediate election event. [11] The cycle implies that its processes are reiterated election after election. The main steps or processes of an election cycle are shown below (they do not necessarily follow sequentially). We do not deal with the use of digital solutions in the campaigning phase (opinion formation issues) as these are qualitatively different from say e-voting, e-registering or e-transmission of results and subject to different requirements.[12]

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

[9] Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation), which became directly applicable across the European Union on 25 May 2018. According to the European Commission, it provides the European Union with the tools necessary to address instances of unlawful use of personal data in the electoral context.
[10] IDEA, *Electoral Management Design*, 2014: 12; 16; 75-77 (minor changes and complements from our side)
[11] See https://www.idea.int/data-tools/tools/online-electoral-cycle
[12] See fn. 5

e. New technologies

"New technologies" refers to "digital" technologies. Several are already used in elections, others are only envisaged or discussed.

The founding layer is the digitization of documents and procedures. Digitization is the conversion of text, pictures, or sound into a digital form that can be processed by a computer. Almost all countries in the region have digitized key election data, including electoral registers, registers of candidates, registers of those who vote, results, etc.[13] Digitized processes include e-registration, e-identification of voters (e-pollbook), e-voting (on voting machines in polling stations or over the internet), e-counting (programmes that register and calculate results and may also allocate seats), statistical analysis, e-transmission of preliminary and/or final results e.g. from polling stations to a central unit, etc. Other technologies include biometry, blockchain, cloud computing, or artificial intelligence. The list is not exhaustive.

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.

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.[14] Its use for voting or registers' administration is discussed. However there is broad agreement in the e-voting IT research community that presently blockchain adds complexity and significant new vulnerabilities without solving any of the challenges of ensuring integrity of elections and it should not be considered for voting.

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.[15] There are public as well as private clouds. Their role in hosting election related data needs to be investigated.

Artificial intelligence (AI) refers to a wide range of methods, both current and speculative.[16] It refers to systems that display intelligent behaviour by analysing their environment and taking action – with some degree of autonomy – to achieve specific goals,[17] including reasoning and decision making, learning and robotics. AI's potential for information retrieving purposes in elections has been mentioned.

Digital technologies introduce new challenges. For instance, *biometry* specifically raises questions such as how unique and permanent are biometrical characteristics to ensure the right to vote over time; how easy and quick is it to collect biometrical information and authenticate the voter prior to voting or whether the collection and use of biometrical characteristics is accepted by voters? *Blockchain* questions the relation between mining power and influence over the process, raises issues of secrecy as a person's identity can be tracked down using public address information and IPs and also given that data posted on the blockchain stays there, questions user-friendliness, as a substantial waiting period is required until a transaction or vote is concluded. When envisaged for voting, another issue is the respect for the requirement of non-publication of intermediary voting results given the fact that the number of votes for each candidate is known before the voting is finished. *Cloud computing* raises questions of security, accountability, interoperability (possibility to

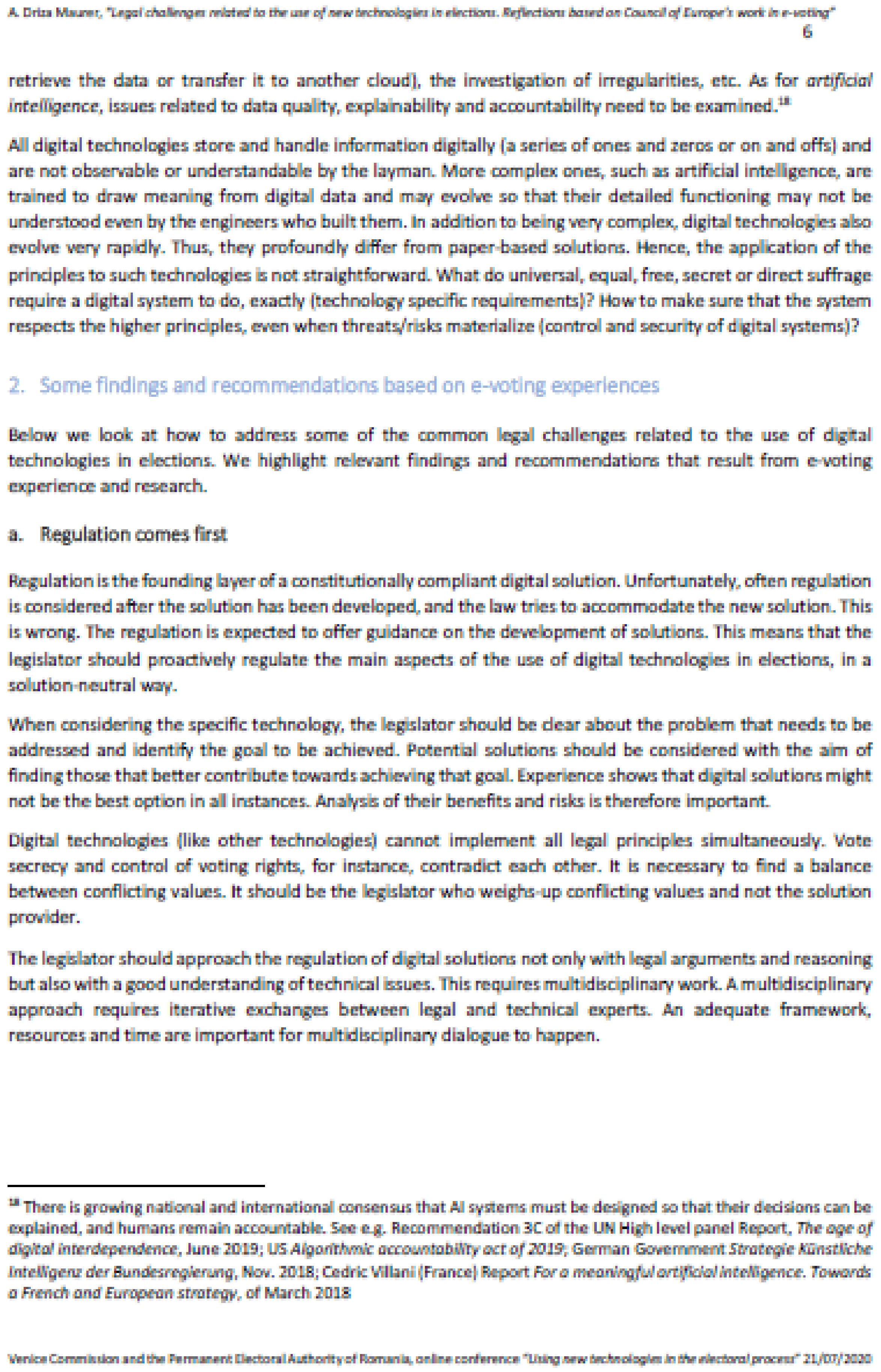
[13] OSCE/ODIHR, *Handbook for the observation of new voting technologies*, 2013

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

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

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

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



retrieve the data or transfer it to another cloud), the investigation of irregularities, etc. As for *artificial intelligence*, issues related to data quality, explainability and accountability need to be examined.[18]

All 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 very complex, digital technologies also evolve very rapidly. Thus, they profoundly differ from paper-based solutions. Hence, the application of the principles to such technologies is not straightforward. What do universal, equal, free, secret or direct suffrage require a digital system to do, exactly (technology specific requirements)? How to make sure that the system respects the higher principles, even when threats/risks materialize (control and security of digital systems)?

2. Some findings and recommendations based on e-voting experiences

Below we look at how to address some of the common legal challenges related to the use of digital technologies in elections. We highlight relevant findings and recommendations that result from e-voting experience and research.

a. Regulation comes first

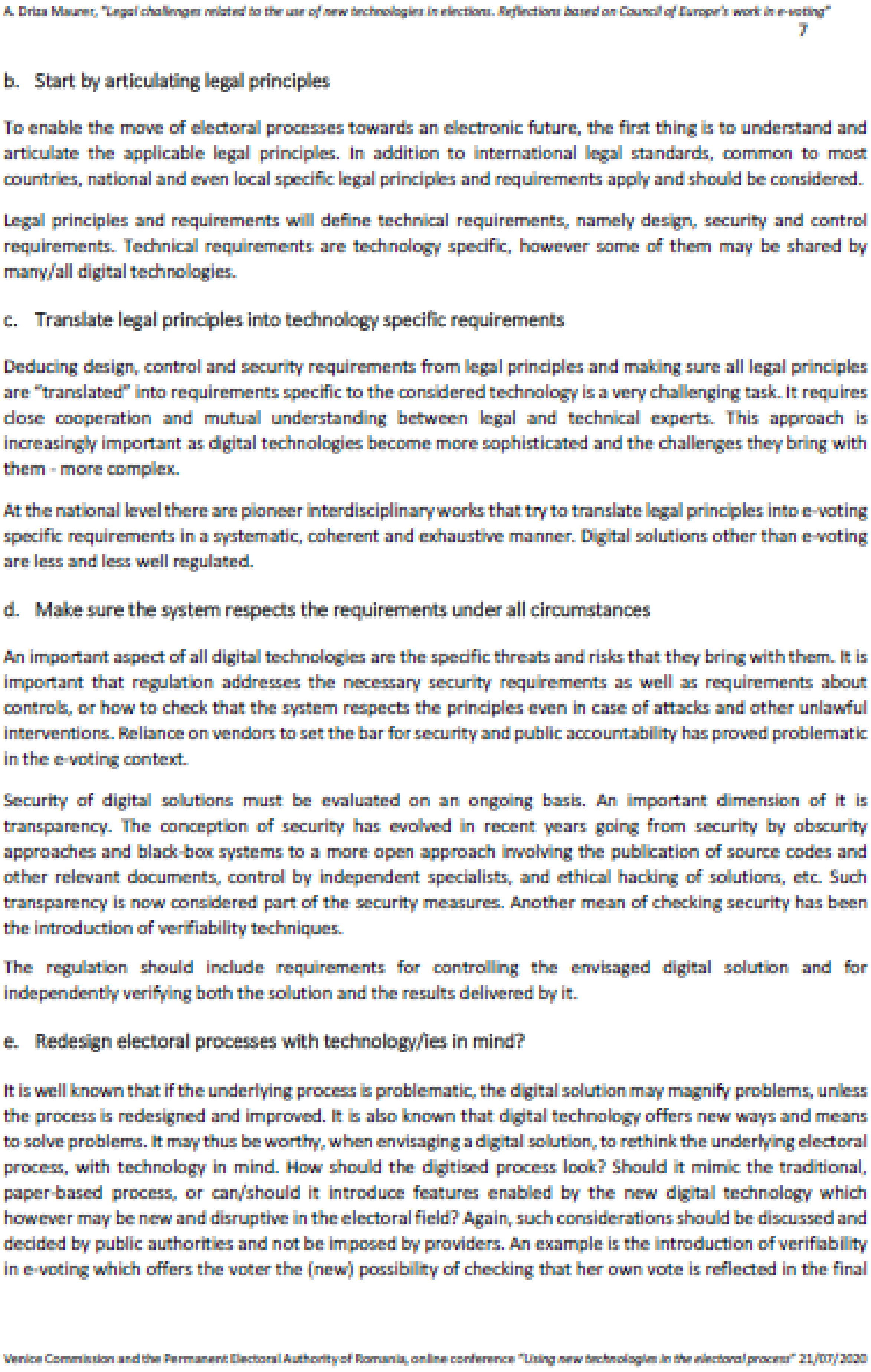
Regulation is the founding layer of a constitutionally compliant digital solution. Unfortunately, often regulation is considered after the solution has been developed, and the law tries to accommodate the new solution. This is wrong. The regulation is expected to offer guidance on the development of solutions. This means that the legislator should proactively regulate the main aspects of the use of digital technologies in elections, in a solution-neutral way.

When considering the specific technology, the legislator should be clear about the problem that needs to be addressed and identify the goal to be achieved. Potential solutions should be considered with the aim of finding those that better contribute towards achieving that goal. Experience shows that digital solutions might not be the best option in all instances. Analysis of their benefits and risks is therefore important.

Digital technologies (like other technologies) cannot implement all legal principles simultaneously. Vote secrecy and control of voting rights, for instance, contradict each other. It is necessary to find a balance between conflicting values. It should be the legislator who weighs-up conflicting values and not the solution provider.

The legislator should approach the regulation of digital solutions not only with legal arguments and reasoning but also with a good understanding of technical issues. This requires multidisciplinary work. A multidisciplinary approach requires iterative exchanges between legal and technical experts. An adequate framework, resources and time are important for multidisciplinary dialogue to happen.

[18] There is growing national and international consensus that AI systems must be designed so that their decisions can be explained, and humans remain accountable. See e.g. Recommendation 3C of the UN High level panel Report, *The age of digital interdependence*, June 2019; US *Algorithmic accountability act of 2019*; German Government *Strategie Künstliche Intelligenz der Bundesregierung*, Nov. 2018; Cedric Villani (France) Report *For a meaningful artificial intelligence. Towards a French and European strategy*, of March 2018



b. Start by articulating legal principles

To enable the move of electoral processes towards an electronic future, the first thing is to understand and articulate the applicable legal principles. In addition to international legal standards, common to most countries, national and even local specific legal principles and requirements apply and should be considered.

Legal principles and requirements will define technical requirements, namely design, security and control requirements. Technical requirements are technology specific, however some of them may be shared by many/all digital technologies.

c. Translate legal principles into technology specific requirements

Deducing design, control and security requirements from legal principles and making sure all legal principles are "translated" into requirements specific to the considered technology is a very challenging task. It requires close cooperation and mutual understanding between legal and technical experts. This approach is increasingly important as digital technologies become more sophisticated and the challenges they bring with them - more complex.

At the national level there are pioneer interdisciplinary works that try to translate legal principles into e-voting specific requirements in a systematic, coherent and exhaustive manner. Digital solutions other than e-voting are less and less well regulated.

d. Make sure the system respects the requirements under all circumstances

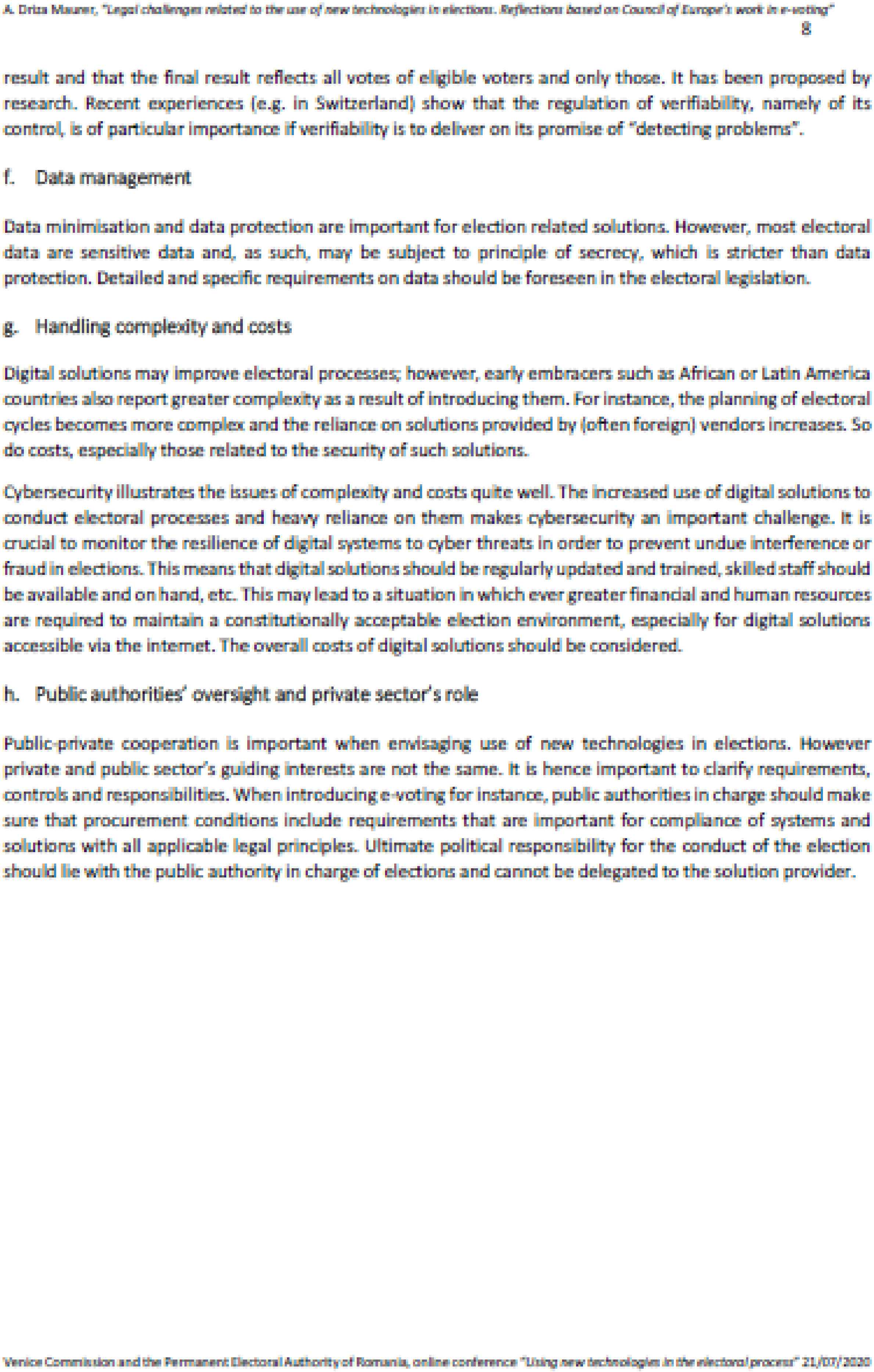
An important aspect of all digital technologies are the specific threats and risks that they bring with them. It is important that regulation addresses the necessary security requirements as well as requirements about controls, or how to check that the system respects the principles even in case of attacks and other unlawful interventions. Reliance on vendors to set the bar for security and public accountability has proved problematic in the e-voting context.

Security of digital solutions must be evaluated on an ongoing basis. An important dimension of it is transparency. The conception of security has evolved in recent years going from security by obscurity approaches and black-box systems to a more open approach involving the publication of source codes and other relevant documents, control by independent specialists, and ethical hacking of solutions, etc. Such transparency is now considered part of the security measures. Another mean of checking security has been the introduction of verifiability techniques.

The regulation should include requirements for controlling the envisaged digital solution and for independently verifying both the solution and the results delivered by it.

e. Redesign electoral processes with technology/ies in mind?

It is well known that if the underlying process is problematic, the digital solution may magnify problems, unless the process is redesigned and improved. It is also known that digital technology offers new ways and means to solve problems. It may thus be worthy, when envisaging a digital solution, to rethink the underlying electoral process, with technology in mind. How should the digitised process look? Should it mimic the traditional, paper-based process, or can/should it introduce features enabled by the new digital technology which however may be new and disruptive in the electoral field? Again, such considerations should be discussed and decided by public authorities and not be imposed by providers. An example is the introduction of verifiability in e-voting which offers the voter the (new) possibility of checking that her own vote is reflected in the final



result and that the final result reflects all votes of eligible voters and only those. It has been proposed by research. Recent experiences (e.g. in Switzerland) show that the regulation of verifiability, namely of its control, is of particular importance if verifiability is to deliver on its promise of "detecting problems".

f. Data management

Data minimisation and data protection are important for election related solutions. However, most electoral data are sensitive data and, as such, may be subject to principle of secrecy, which is stricter than data protection. Detailed and specific requirements on data should be foreseen in the electoral legislation.

g. Handling complexity and costs

Digital solutions may improve electoral processes; however, early embracers such as African or Latin America countries also report greater complexity as a result of introducing them. For instance, the planning of electoral cycles becomes more complex and the reliance on solutions provided by (often foreign) vendors increases. So do costs, especially those related to the security of such solutions.

Cybersecurity illustrates the issues of complexity and costs quite well. The increased use of digital solutions to conduct electoral processes and heavy reliance on them makes cybersecurity an important challenge. It is crucial to monitor the resilience of digital systems to cyber threats in order to prevent undue interference or fraud in elections. This means that digital solutions should be regularly updated and trained, skilled staff should be available and on hand, etc. This may lead to a situation in which ever greater financial and human resources are required to maintain a constitutionally acceptable election environment, especially for digital solutions accessible via the internet. The overall costs of digital solutions should be considered.

h. Public authorities' oversight and private sector's role

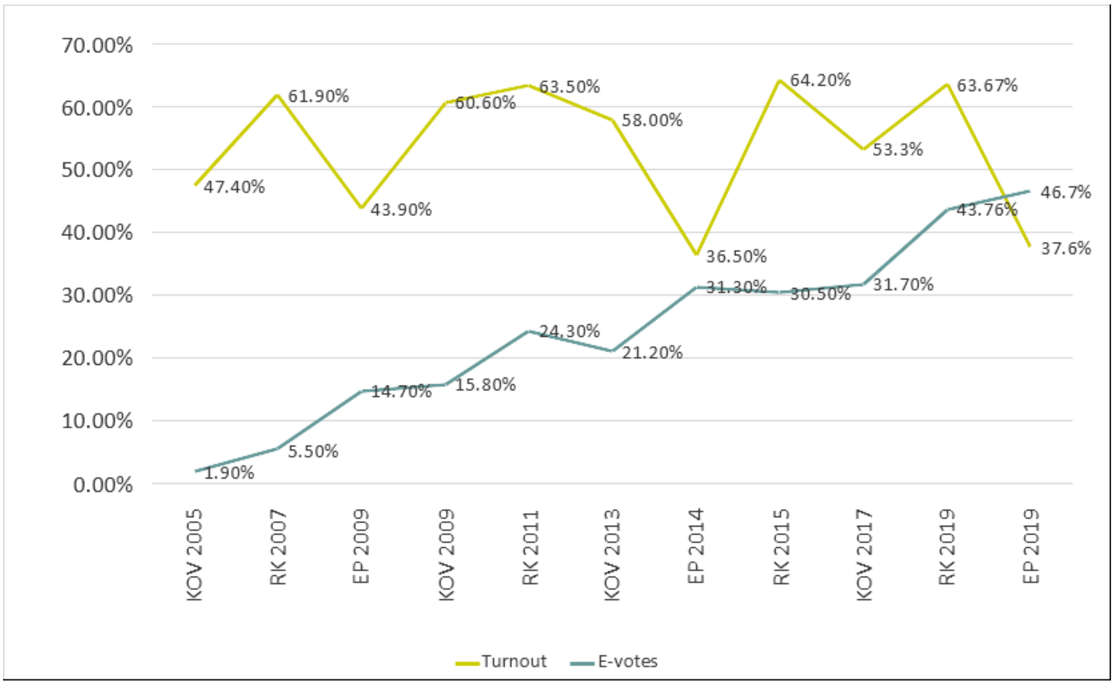
Public-private cooperation is important when envisaging use of new technologies in elections. However private and public sector's guiding interests are not the same. It is hence important to clarify requirements, controls and responsibilities. When introducing e-voting for instance, public authorities in charge should make sure that procurement conditions include requirements that are important for compliance of systems and solutions with all applicable legal principles. Ultimate political responsibility for the conduct of the election should lie with the public authority in charge of elections and cannot be delegated to the solution provider.

Report by Mr T. Martens

I-voting in Estonia

Electronic voting (i-voting) allows votes to be cast via the Internet. A computer with an Internet connection and an ID-card or mobile ID with valid certificates are needed for that. In elections, i-voting is open for the whole duration of the advance voting period.

Estonia was the first country in the world to implement i-voting in national elections. Electronic voting with binding results has been carried out in Estonia since 2005. I-voting is popular primarily because it is efficient and convenient. Today, almost half of votes are cast via the Internet. The i-voting system currently used was completed by local elections of 2017, and it has been developed according to the new electronic voting framework.



1. The i-voting procedure

I-voting is organised by the State Electoral Office in cooperation with the Information System Authority. Before the beginning of voting, the State Electoral Office prepares the i-voting system and discloses the voter application necessary for voting on the website “valimised.ee”.

Electronic voting is open twenty-four hours on all days of advance voting (from the tenth to the fourth day before election day).

The following are needed for i-voting:

- a computer connected to the Internet;
- an ID-card, mobile ID or digital identity document with valid certificates and PIN codes.

For i-voting, the voter application needs to be downloaded to the computer. The voter application automatically checks the voter’s eligibility to vote and displays a correct list of candidates to the voter. After a choice has been made, the voter application encrypts the voter’s vote. The voter confirms the voting with their digital signature, and the voter application forwards the vote to the vote collecting server. At the same time, the independent registration service provides every vote with a time stamp which allows to verify later that all votes have indeed been forwarded to the collector.

The voter can check if their vote has been forwarded and received correctly with a separate smart device application.
T. Martens, Estonia's experience with e-voting

I-votes are encrypted, using a suitable and up-to-date crypto-algorithm. The precise specification of the algorithm is determined by the State Electoral Office every time before elections. A vote is encrypted with the help of two encryption keys. The voter application uses a public vote encryption key. The vote-opening key is needed to open a vote; only members of the National Electoral Committee have access to the key.

2. Changing of an i-vote

I-voting does not take place in a controlled environment like a polling place. In order to ensure that the voter expresses their actual will, it is possible for them to change their vote cast electronically.

During i-voting, a voter can always vote again and change their vote as many times as they wish. Only the last i-vote cast is taken into account, and earlier votes are annulled.

A voter may also vote by ballot paper in a voting district during advance voting. A vote cast on a ballot paper in a voting district is final (it is impossible to retrieve it from the ballot box), and therefore in such a case all i-votes of the voter are annulled. Before election day, the voting district committee receives a list of voters who have voted electronically, and compares it against the list of voters of its district on paper. If there is a notation or signature in the list concerning voting by a voter, the voting district committee submits a notice to the State Electoral Office to annul the i-vote.

I-votes are annulled on Sunday immediately before the counting of votes cast electronically. A voter cannot change their I-vote on the election day.

3. Counting of i-votes and verification of results

The State Electoral Office ascertains the results of i-voting in the evening of election day. The procedure is public, and observers and members of the National Electoral Committee are present.

In the counting of e-votes, the following acts are performed with the votes:

1. all i-votes that have to be annulled due to changing of i-votes are annulled;
2. the personal data (digital signatures) of voters are separated from electronic votes. Anonymous votes are subject to counting. An i-vote contains only the election identificator, and a candidate registration number;
3. i-votes are opened, using the vote-opening key. Access to the key is distributed between the members of the National Electoral Committee;
4. votes are counted and the number of votes cast for candidates is ascertained;
5. the voting results are entered into the election information system.

The results of electronic voting are not published until the end of voting on election day (after 8 p.m. in Riigikogu election).

After the counting of i-votes (as a rule, on the following day), the integrity of i-votes is checked. Put simply, it can be described as the second recounting of i-votes. In order for the counting of votes to be publicly verifiable, electronic votes are mixed and rearranged. Mixing must be carried out in such a way that the decryption of both the input and the output would give the same result. In the course of data audit, the auditor also checks the integrity of the i-ballot box, and the correctness of the annulment of repeated votes and of the anonymisation of votes. On the same bases with the auditor, observers can also carry out similar checking procedures.

T. Martens, Estonia's experience with e-voting

4. Ensuring free elections and secrecy of voting in i-voting

Section 60 of the Constitution provides that elections are free, general, uniform and direct, and that voting is secret. All manners of voting must be in compliance with these principles. In i-voting, too, it must be ensured that voting takes place freely and that i-votes remain secret.

Voters are not always in the same situation when using different manners of voting, and therefore the measures to ensure the secrecy of votes and free elections in i-voting are also different from those used in ordinary voting. Differently from the voting in a voting district in the environment controlled by the electoral committee, an i-voter votes independently, choosing the time and place convenient to them. An e-voter votes by himself or herself. Voting by using another person's ID card or mobile ID, as well as transfer of the codes thereof to another person is not allowed. In order to avoid the risks related to the security of the computer, a computer which belongs to the voter or to a reliable person must be used in i-voting.

If a voter finds that they were influenced during the casting of i-vote, they do not trust the computer they are using, or they could not vote in secrecy, it is always possible for them to change their vote as many times as they wish during the advance voting period. The last vote cast is taken into account. Therefore, if anyone wishes a voter to vote in a certain manner, it is not possible for them to check it, because they cannot know the voter's choice when casting the last i-vote.

Besides, it is possible for a voter to vote by paper ballot in a voting district during advance voting. In such a case, their i-vote is annulled, and the vote cast on a ballot paper is taken into account.

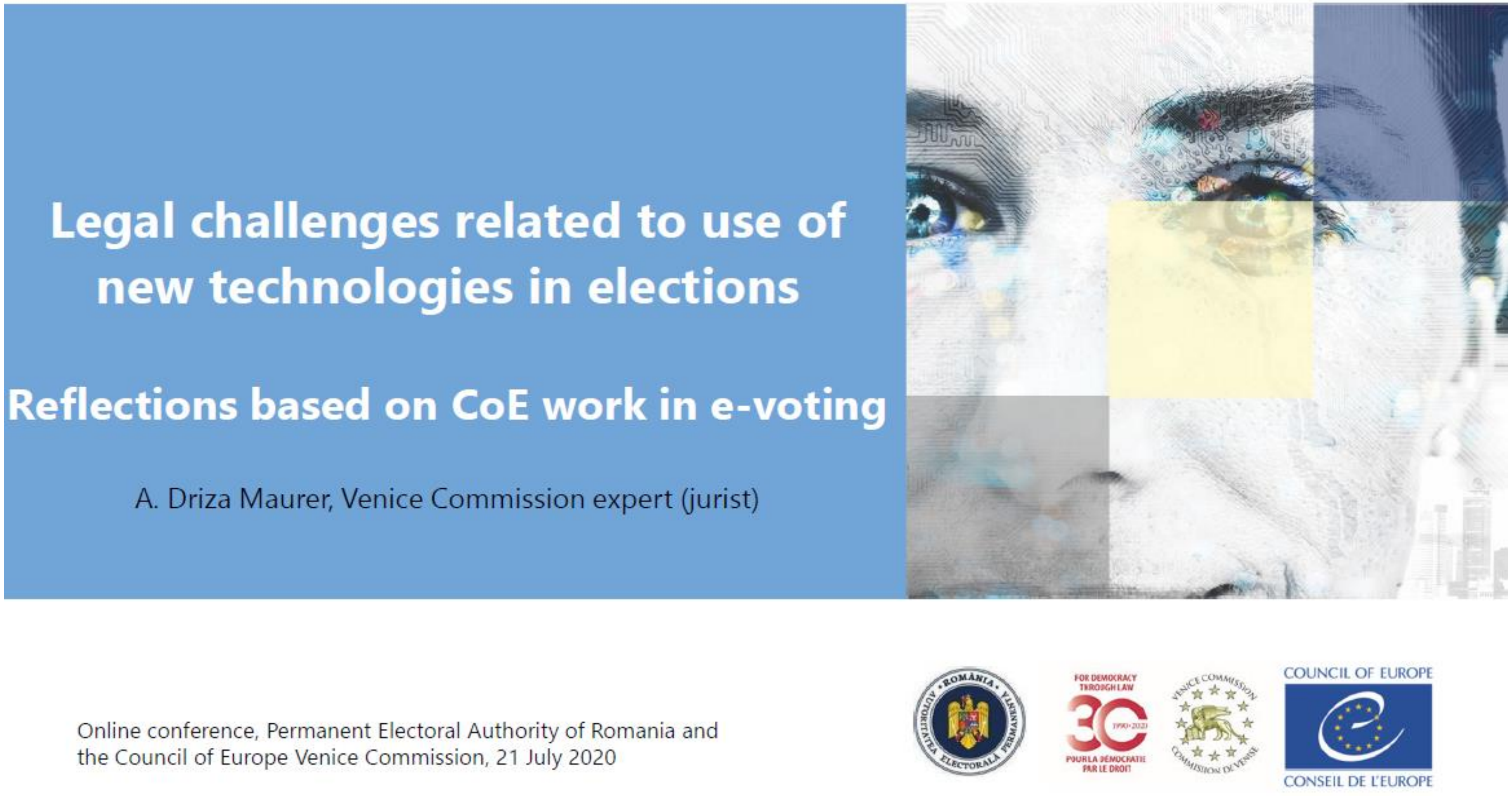
Encryption ensures the secrecy of i-votes in the forwarding of votes. Also, the i-voting system separates personal data from i-votes before the counting of votes, and the anonymised votes are counted.

Ensuring the uniformity of elections, and equal treatment of voters in i-voting

The principle of uniformity means that the vote of every voter must have the same weight in elections. In electronic voting, a voter is in a different situation compared to voting in a voting district, because it is possible for the voter to change their i-vote, but not the vote cast on a ballot paper. Therefore the question may arise whether a voter who votes electronically has an advantage over a voter who votes by ballot. The Supreme Court has also assessed that. In 2005, the Supreme Court found that, in i-voting, despite the repeated voting, a voter has no possibility to affect the election results to a greater degree than the voters who use other manners of voting[1]. A vote cast by electronic means is counted as one vote, and in terms of election results, it does not have more influence than a vote cast by a voter using another manner of voting. The Supreme Court also found that the principle of equal treatment in the context of electing representative bodies does not mean that absolutely equal possibilities for performing the voting act in equal manner should be guaranteed to all persons with the right to vote.

[1] Judgment No 3-4-1-13-05 of 1 September 2005 of the Constitutional Review Chamber of the Supreme Court (in Estonian)

Appendix I



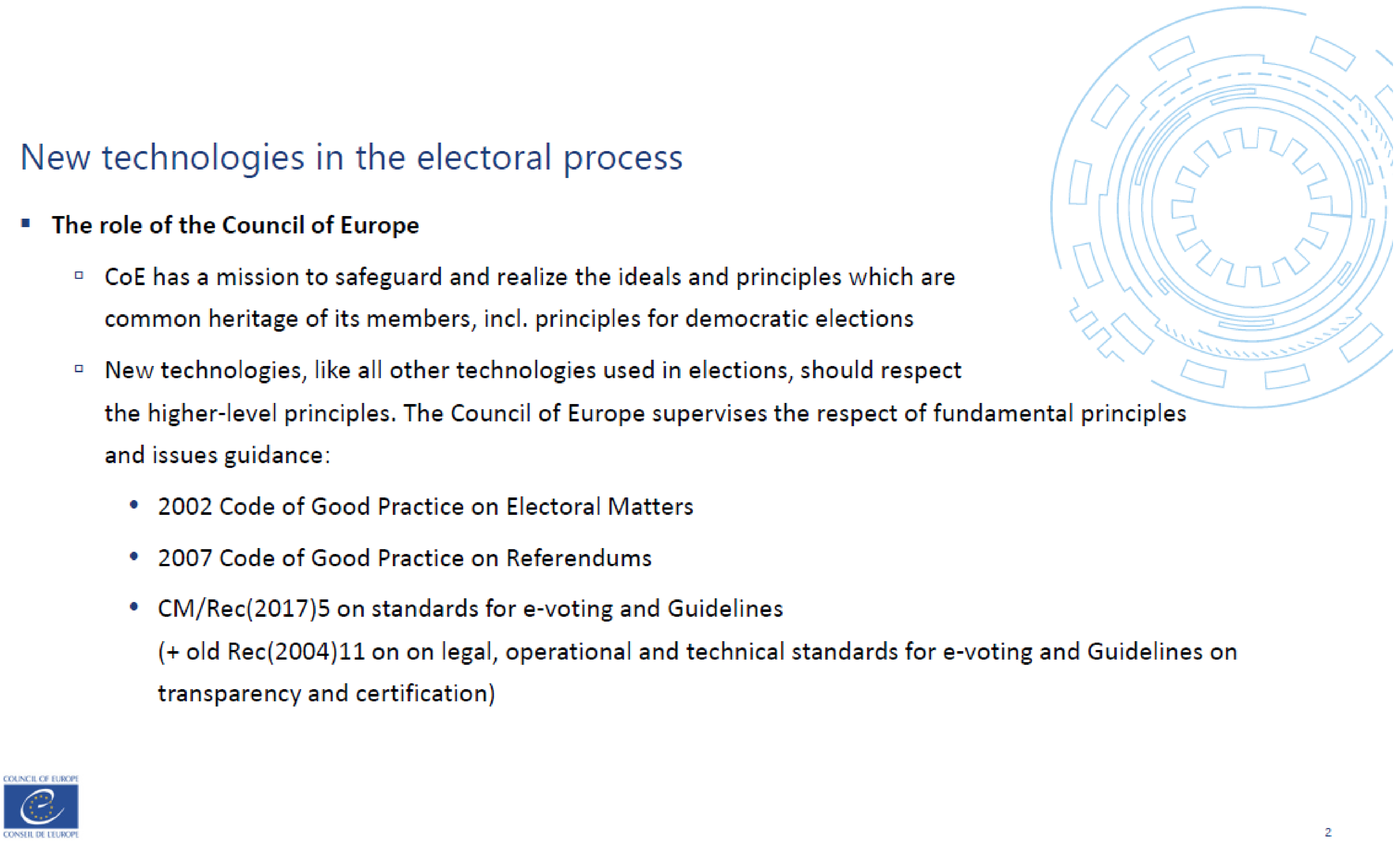
Legal challenges related to use of new technologies in elections

Reflections based on CoE work in e-voting

A. Driza Maurer, Venice Commission expert (jurist)

Online conference, Permanent Electoral Authority of Romania and the Council of Europe Venice Commission, 21 July 2020

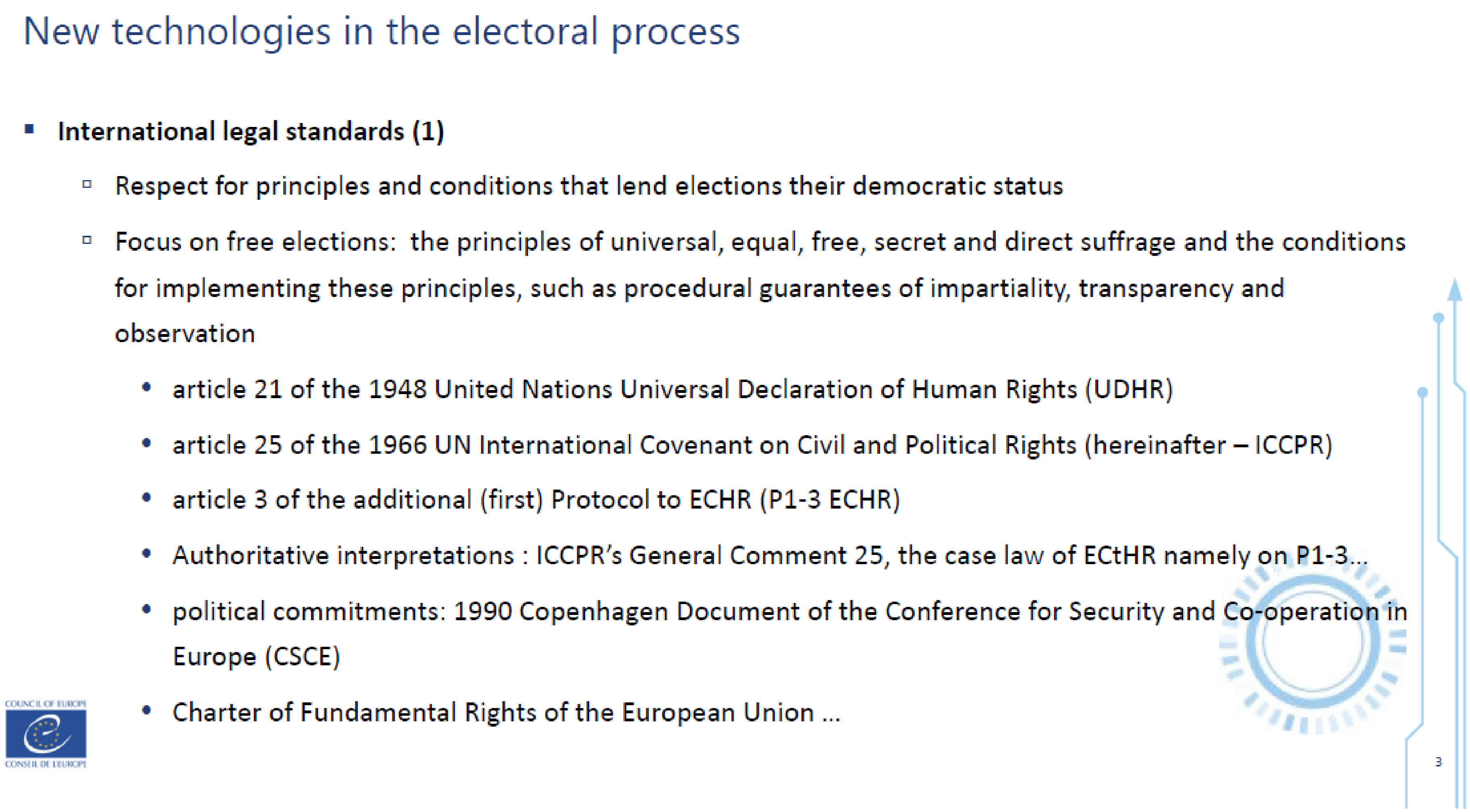
ROMÂNIA AUTORITATEA ELECTORALĂ PERMANENTĂ
FOR DEMOCRACY THROUGH LAW
30
1990-2020
POUR LA DÉMOCRATIE PAR LE DROIT
VENICE COMMISSION
COMMISSION DE VENISE
COUNCIL OF EUROPE
CONSEIL DE L'EUROPE



New technologies in the electoral process

- **The role of the Council of Europe**
  - CoE has a mission to safeguard and realize the ideals and principles which are common heritage of its members, incl. principles for democratic elections
  - New technologies, like all other technologies used in elections, should respect the higher-level principles. The Council of Europe supervises the respect of fundamental principles and issues guidance:
    - 2002 Code of Good Practice on Electoral Matters
    - 2007 Code of Good Practice on Referendums
    - CM/Rec(2017)5 on standards for e-voting and Guidelines (+ old Rec(2004)11 on on legal, operational and technical standards for e-voting and Guidelines on transparency and certification)

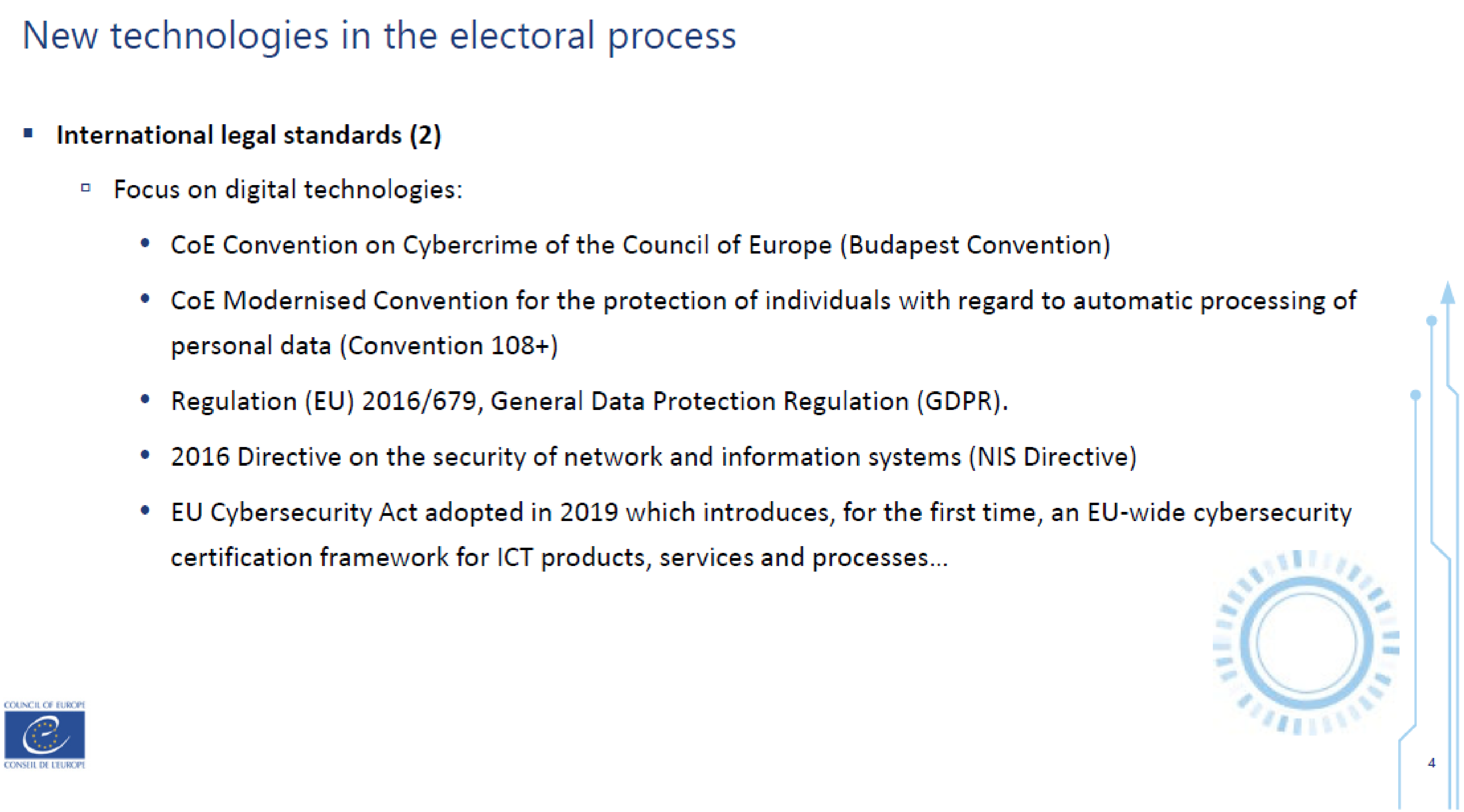
2



New technologies in the electoral process

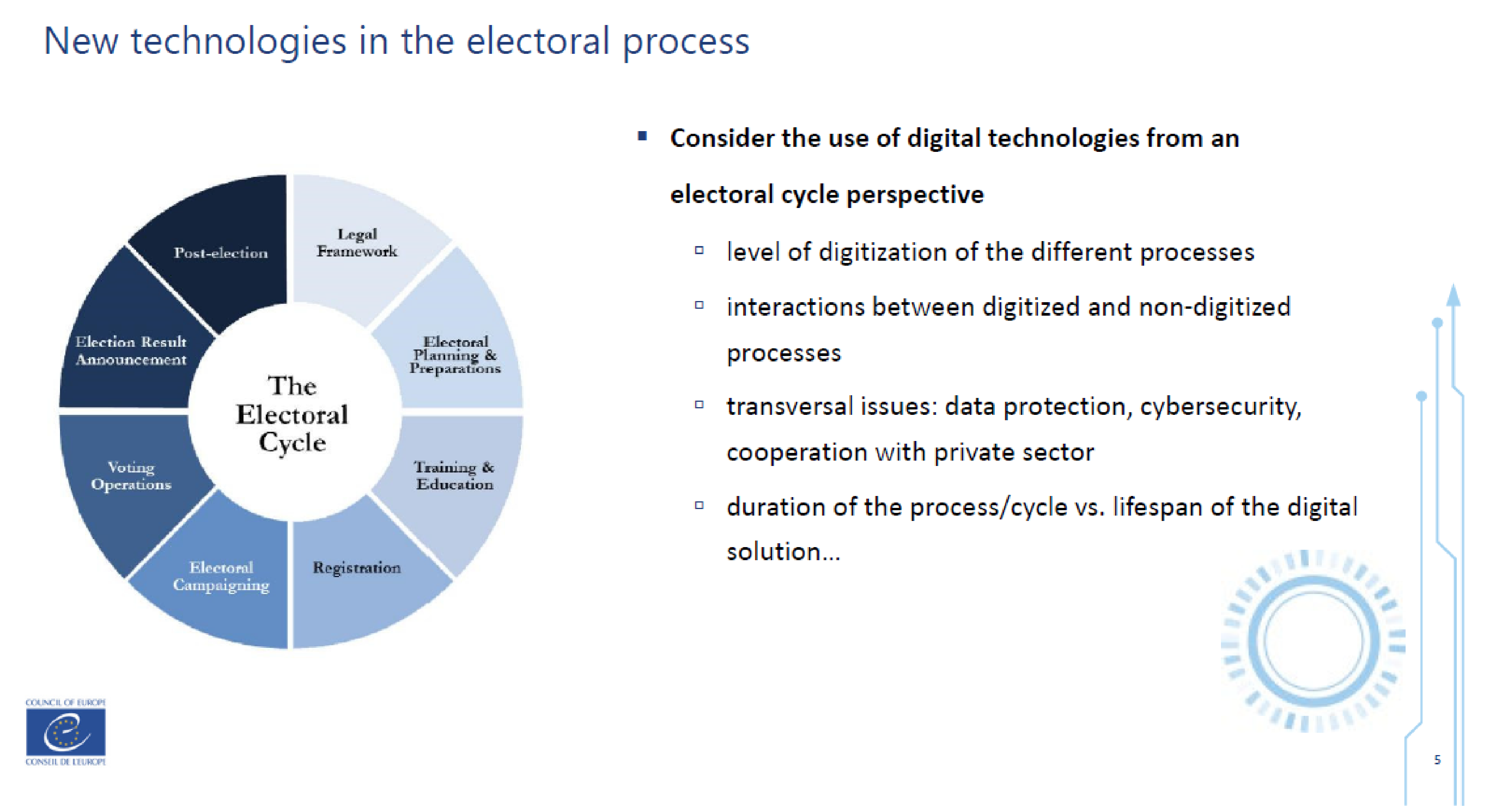
- **International legal standards (1)**
  - Respect for principles and conditions that lend elections their democratic status
  - Focus on free elections: the principles of universal, equal, free, secret and direct suffrage and the conditions for implementing these principles, such as procedural guarantees of impartiality, transparency and observation
    - article 21 of the 1948 United Nations Universal Declaration of Human Rights (UDHR)
    - article 25 of the 1966 UN International Covenant on Civil and Political Rights (hereinafter – ICCPR)
    - article 3 of the additional (first) Protocol to ECHR (P1-3 ECHR)
    - Authoritative interpretations : ICCPR's General Comment 25, the case law of ECtHR namely on P1-3…
    - political commitments: 1990 Copenhagen Document of the Conference for Security and Co-operation in Europe (CSCE)
    - Charter of Fundamental Rights of the European Union …

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE



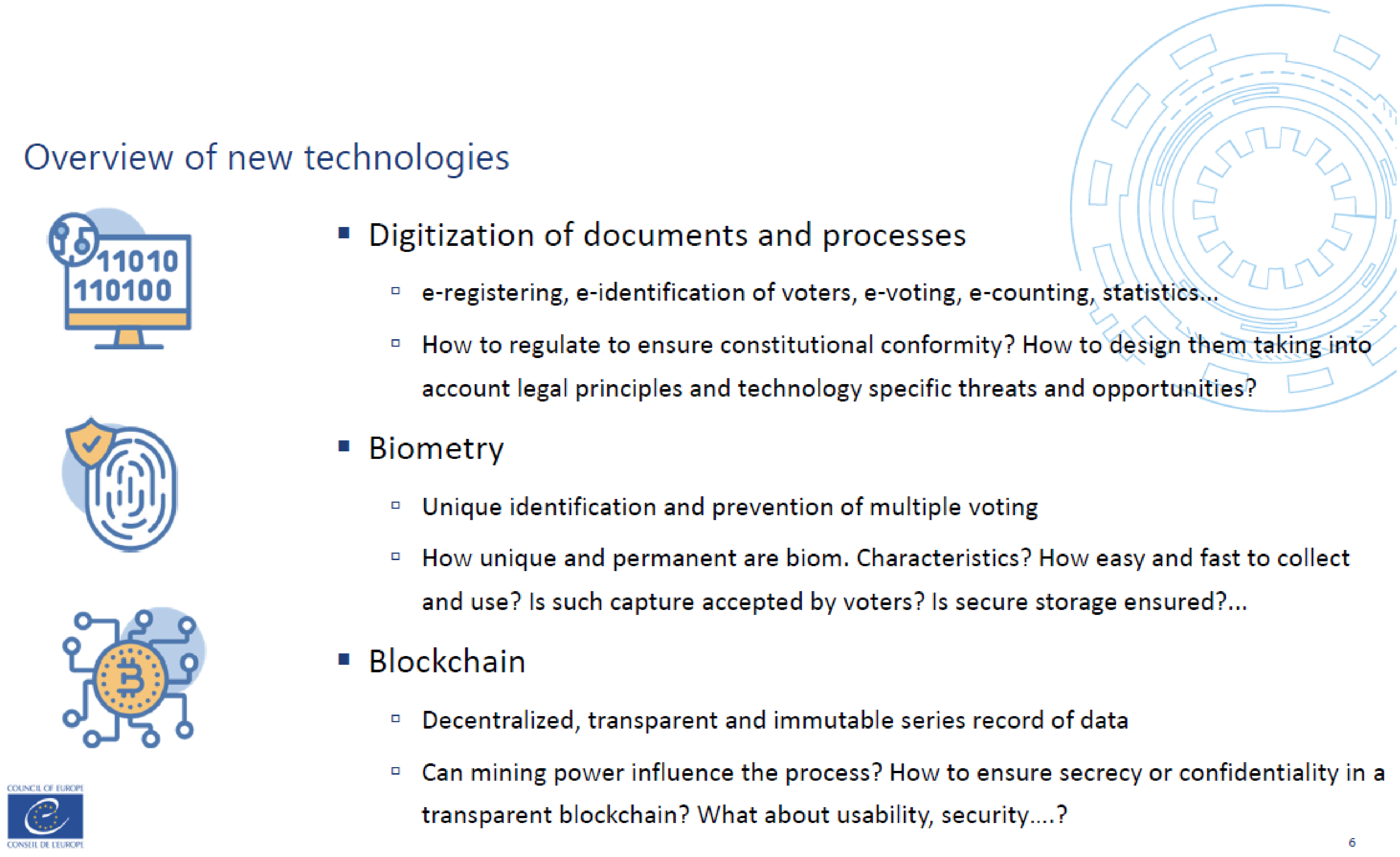
New technologies in the electoral process

- **International legal standards (2)**
  - Focus on digital technologies:
    - CoE Convention on Cybercrime of the Council of Europe (Budapest Convention)
    - CoE Modernised Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108+)
    - Regulation (EU) 2016/679, General Data Protection Regulation (GDPR).
    - 2016 Directive on the security of network and information systems (NIS Directive)
    - EU Cybersecurity Act adopted in 2019 which introduces, for the first time, an EU-wide cybersecurity certification framework for ICT products, services and processes…



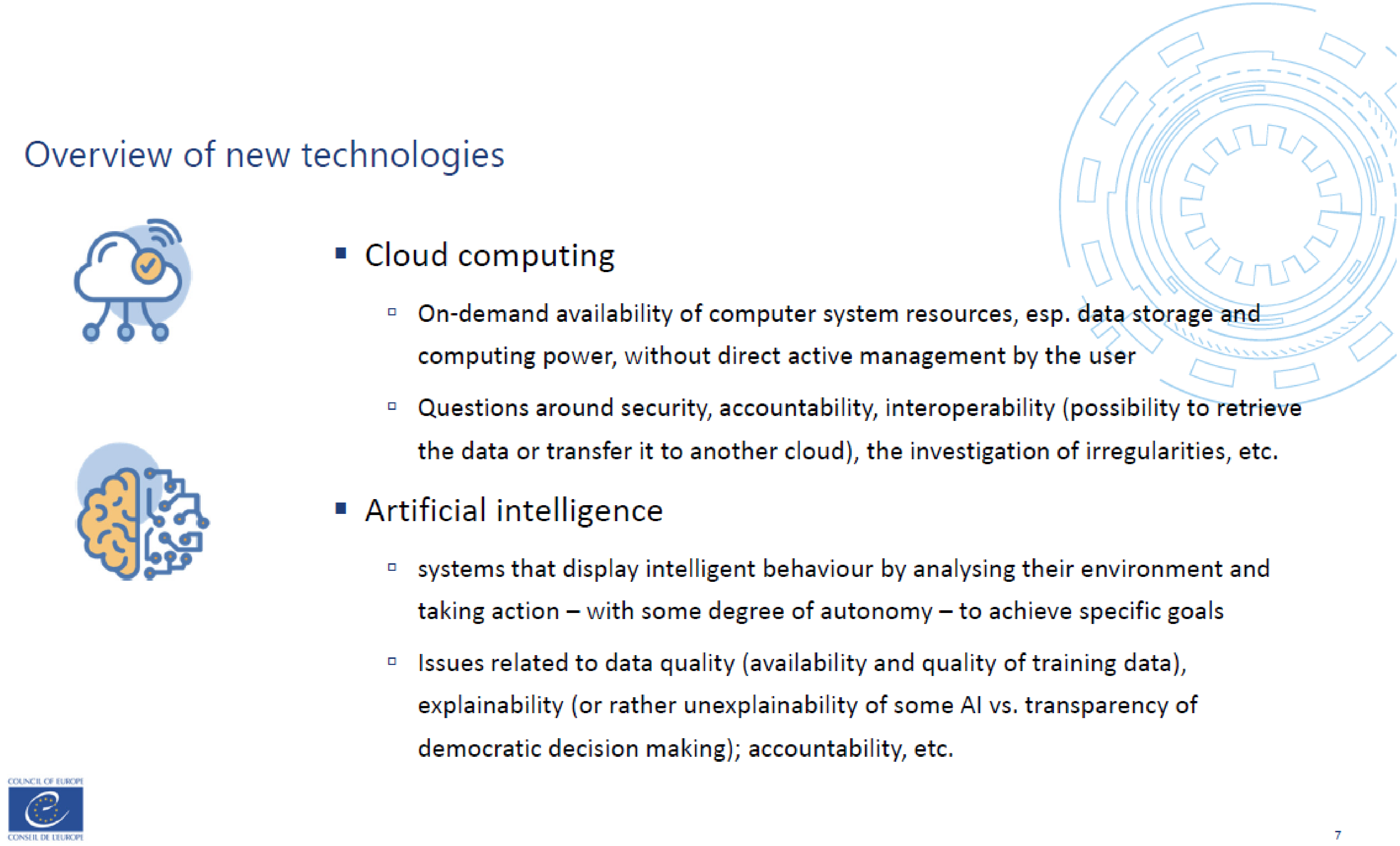
New technologies in the electoral process

- **Consider the use of digital technologies from an electoral cycle perspective**
  - level of digitization of the different processes
  - interactions between digitized and non-digitized processes
  - transversal issues: data protection, cybersecurity, cooperation with private sector
  - duration of the process/cycle vs. lifespan of the digital solution…



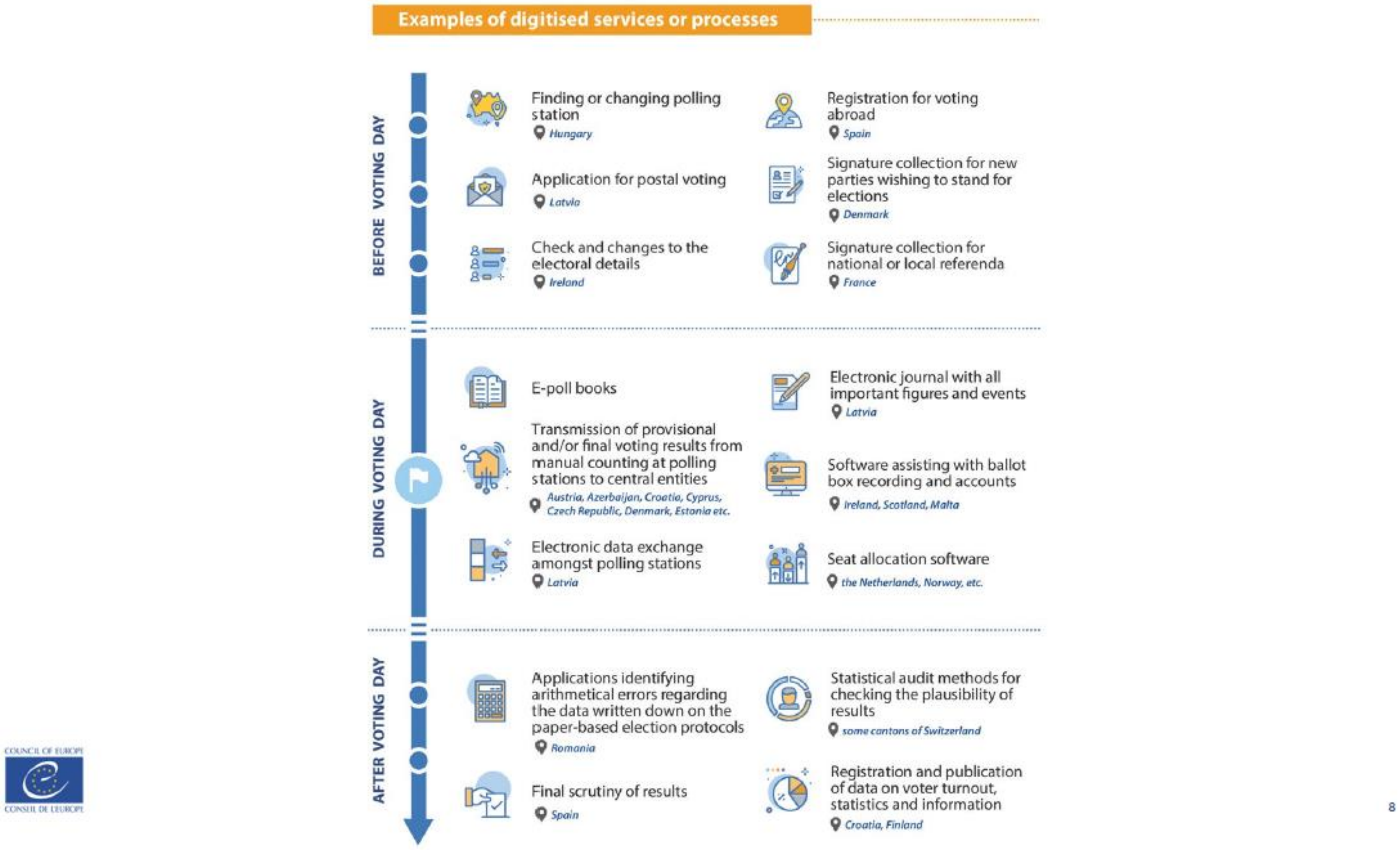
Overview of new technologies

- Digitization of documents and processes
  - e-registering, e-identification of voters, e-voting, e-counting, statistics…
  - How to regulate to ensure constitutional conformity? How to design them taking into account legal principles and technology specific threats and opportunities?
- Biometry
  - Unique identification and prevention of multiple voting
  - How unique and permanent are biom. Characteristics? How easy and fast to collect and use? Is such capture accepted by voters? Is secure storage ensured?…
- Blockchain
  - Decentralized, transparent and immutable series record of data
  - Can mining power influence the process? How to ensure secrecy or confidentiality in a transparent blockchain? What about usability, security….?



Overview of new technologies

- Cloud computing
  - On-demand availability of computer system resources, esp. data storage and computing power, without direct active management by the user
  - Questions around security, accountability, interoperability (possibility to retrieve the data or transfer it to another cloud), the investigation of irregularities, etc.
- Artificial intelligence
  - systems that display intelligent behaviour by analysing their environment and taking action – with some degree of autonomy – to achieve specific goals
  - Issues related to data quality (availability and quality of training data), explainability (or rather unexplainability of some AI vs. transparency of democratic decision making); accountability, etc.



Examples of digitised services or processes

BEFORE VOTING DAY

Finding or changing polling station
Hungary

Registration for voting abroad
Spain

Application for postal voting
Latvia

Signature collection for new parties wishing to stand for elections
Denmark

Check and changes to the electoral details
Ireland

Signature collection for national or local referenda
France

DURING VOTING DAY

E-poll books

Electronic journal with all important figures and events
Latvia

Transmission of provisional and/or final voting results from manual counting at polling stations to central entities
Austria, Azerbaijan, Croatia, Cyprus, Czech Republic, Denmark, Estonia etc.

Software assisting with ballot box recording and accounts
Ireland, Scotland, Malta

Electronic data exchange amongst polling stations
Latvia

Seat allocation software
the Netherlands, Norway, etc.

AFTER VOTING DAY

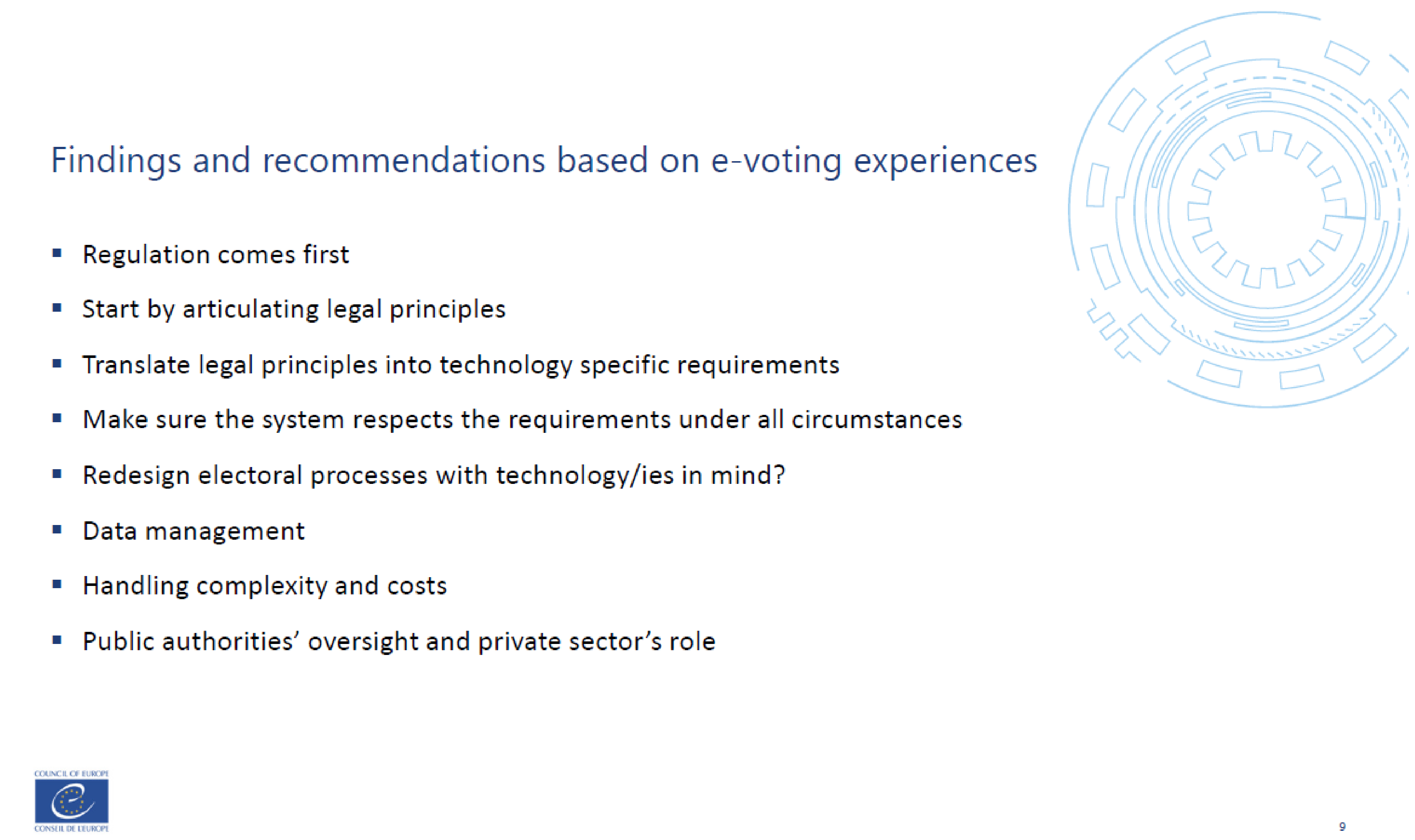
Applications identifying arithmetical errors regarding the data written down on the paper-based election protocols
Romania

Statistical audit methods for checking the plausibility of results
some cantons of Switzerland

Final scrutiny of results
Spain

Registration and publication of data on voter turnout, statistics and information
Croatia, Finland

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE



Findings and recommendations based on e-voting experiences

- Regulation comes first
- Start by articulating legal principles
- Translate legal principles into technology specific requirements
- Make sure the system respects the requirements under all circumstances
- Redesign electoral processes with technology/ies in mind?
- Data management
- Handling complexity and costs
- Public authorities’ oversight and private sector’s role

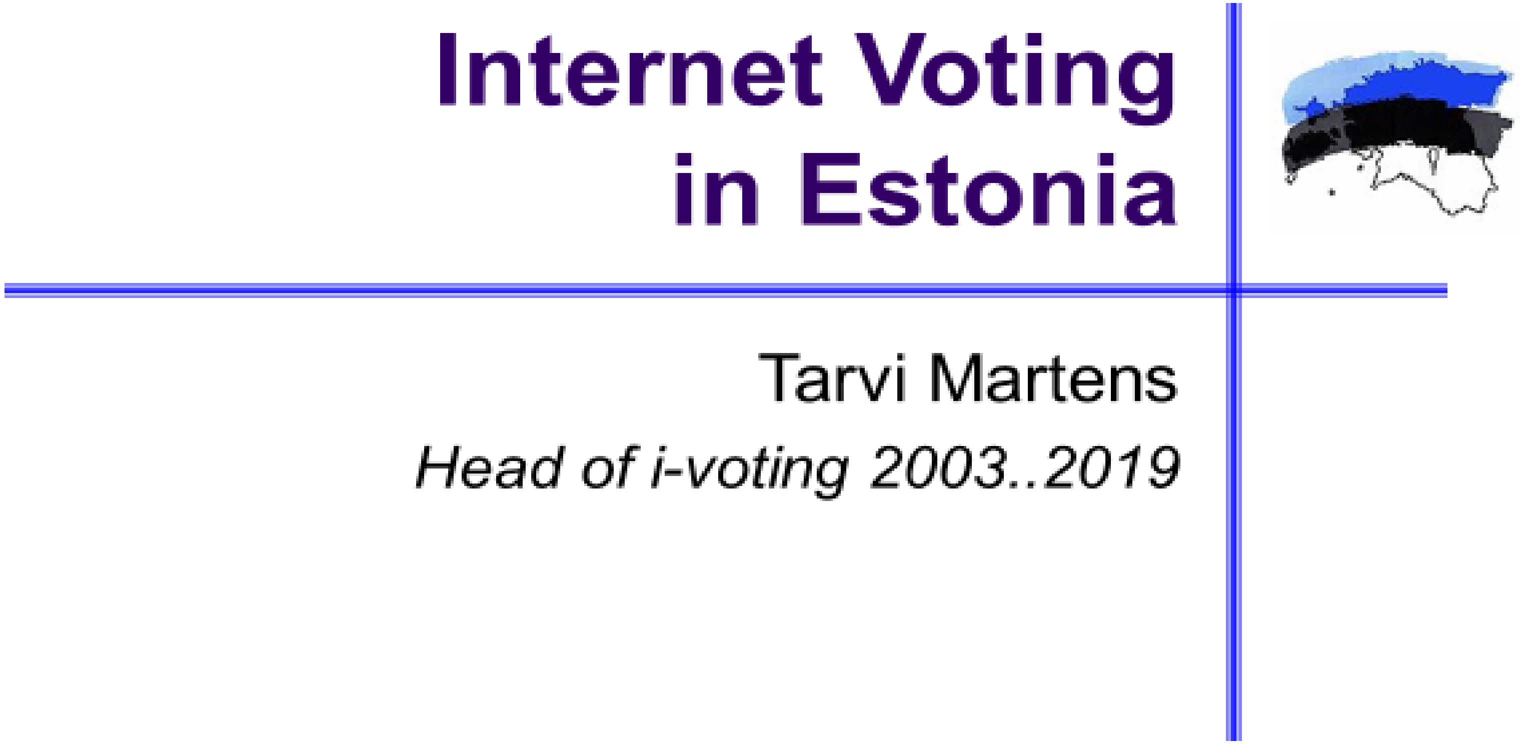
See also: A. Driza Maurer, *Digital Technologies in Elections. Questions, lessons learned, perspectives*

Council of Europe website, June 2020

Thank you for your attention!

ardita.drizamaurer@uzh.ch

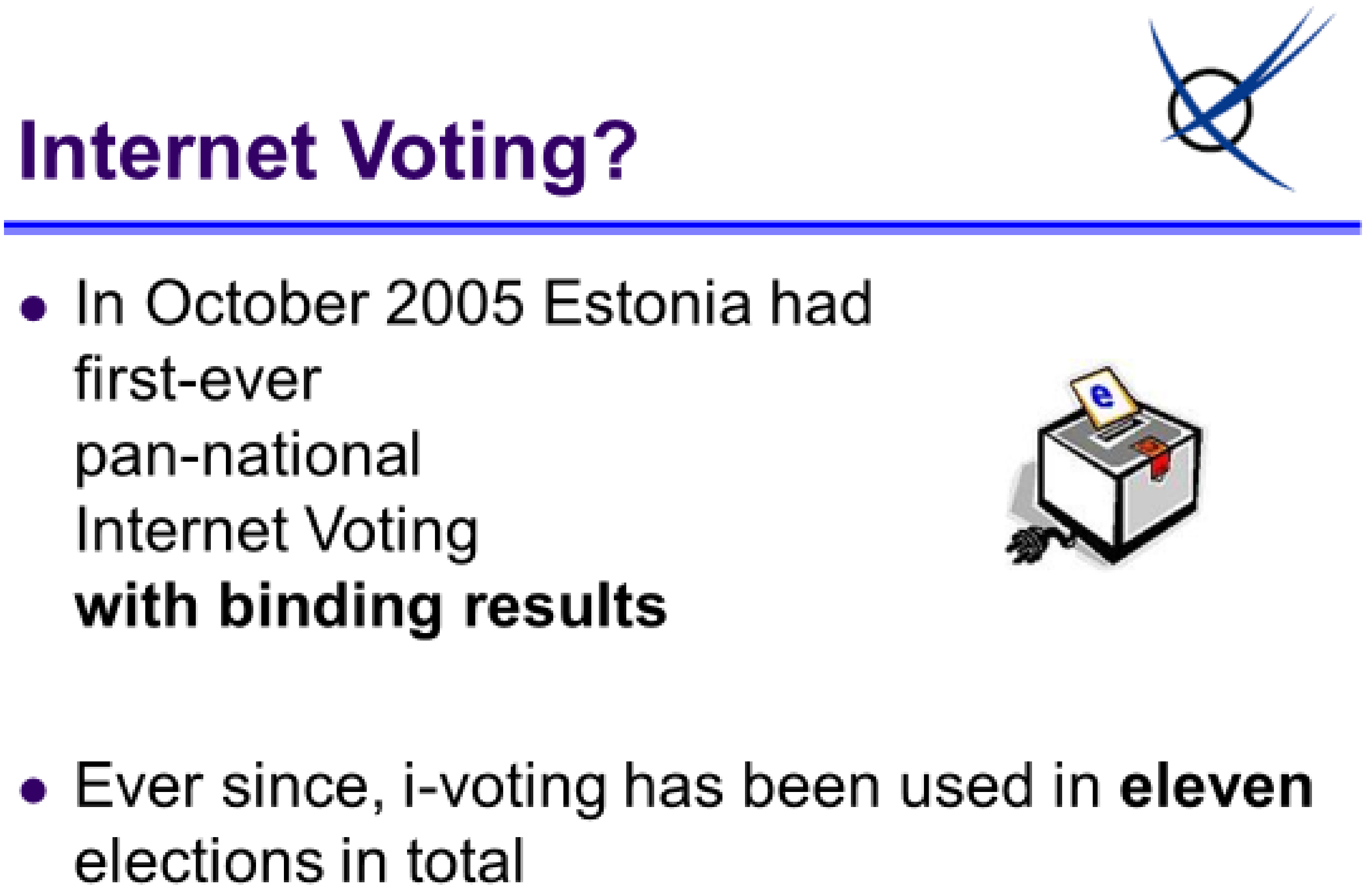
Appendix II



Internet Voting in Estonia

Tarvi Martens

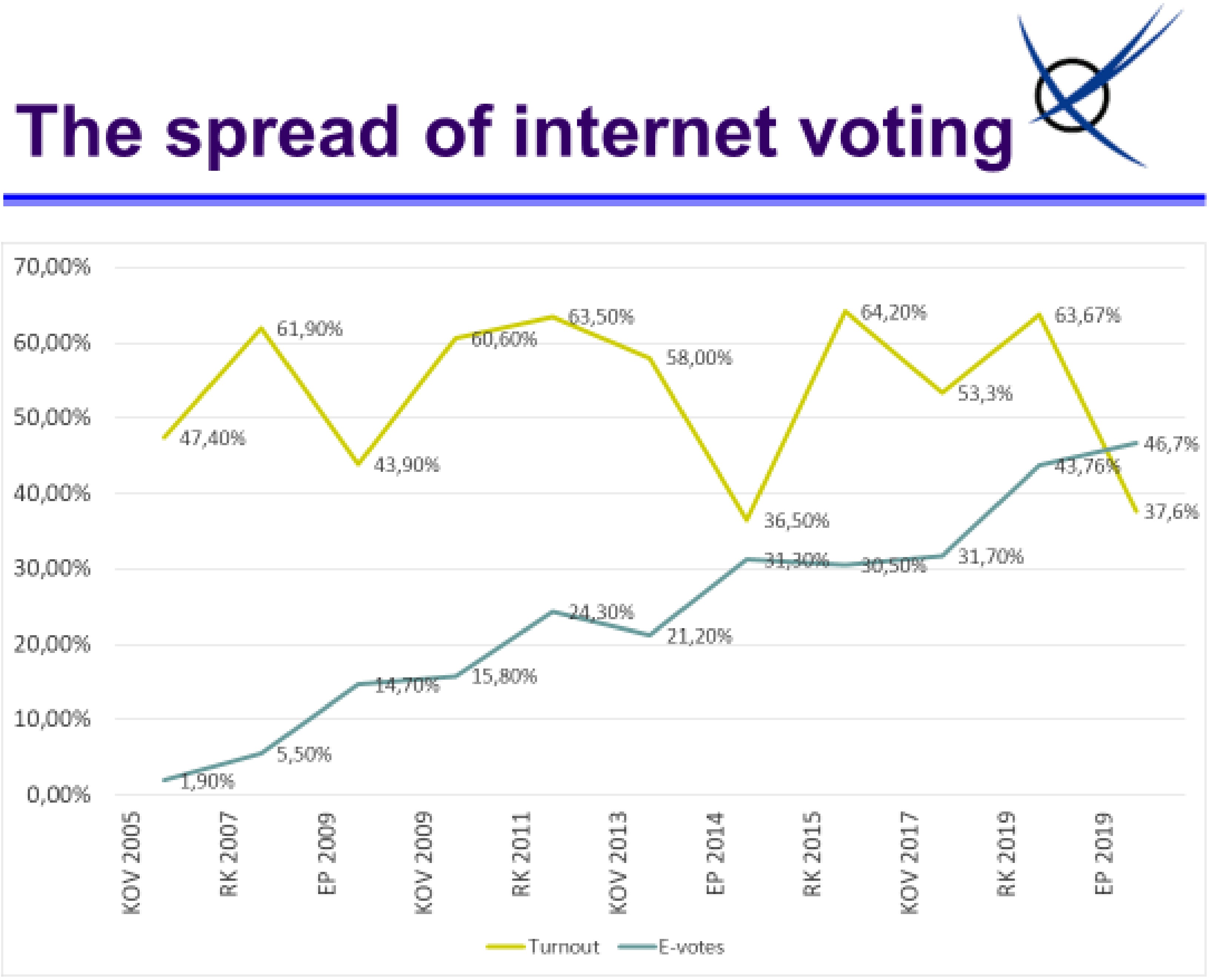
Head of i-voting 2003..2019



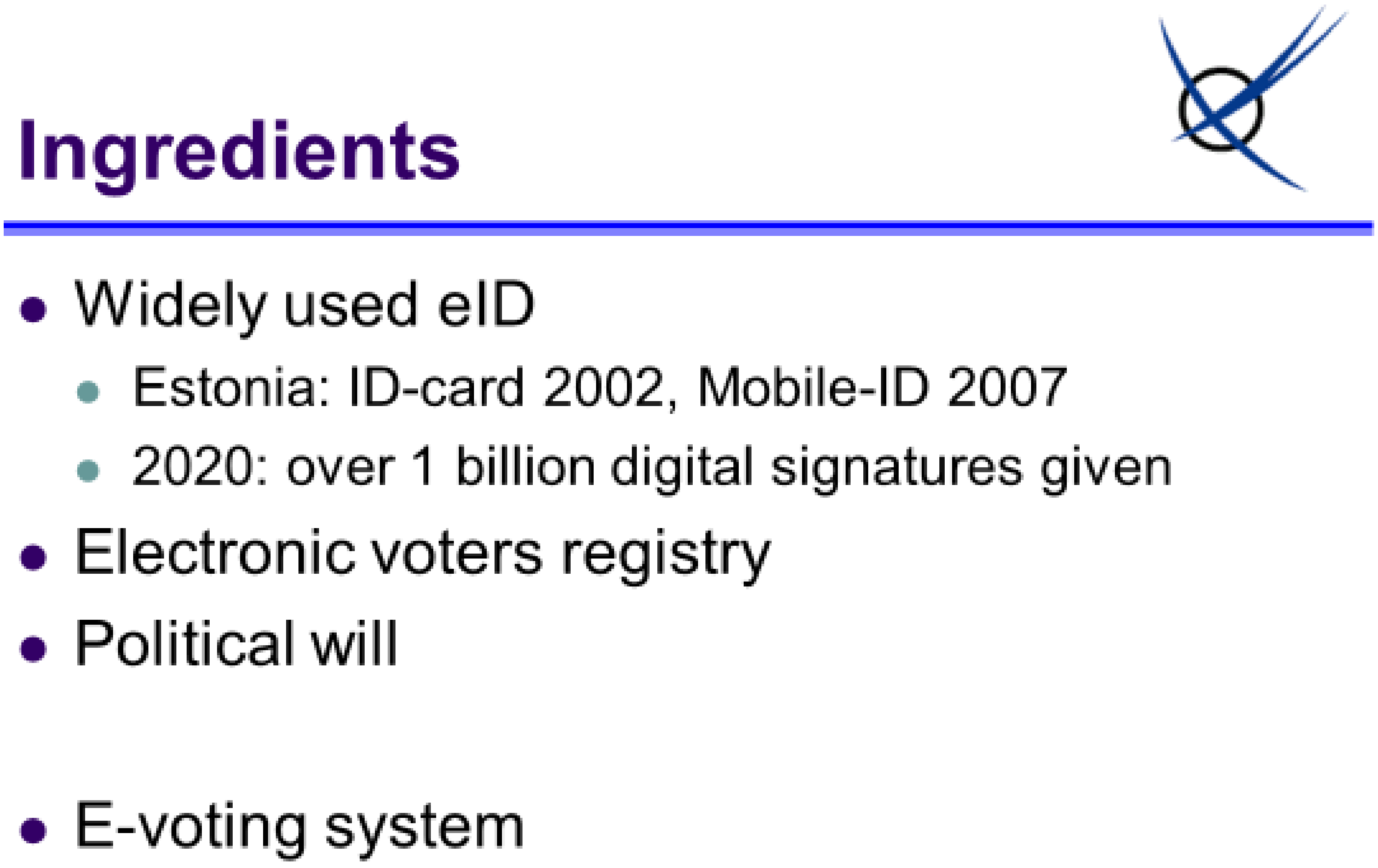
Internet Voting?

- In October 2005 Estonia had first-ever pan-national Internet Voting **with binding results**

- Ever since, i-voting has been used in **eleven** elections in total



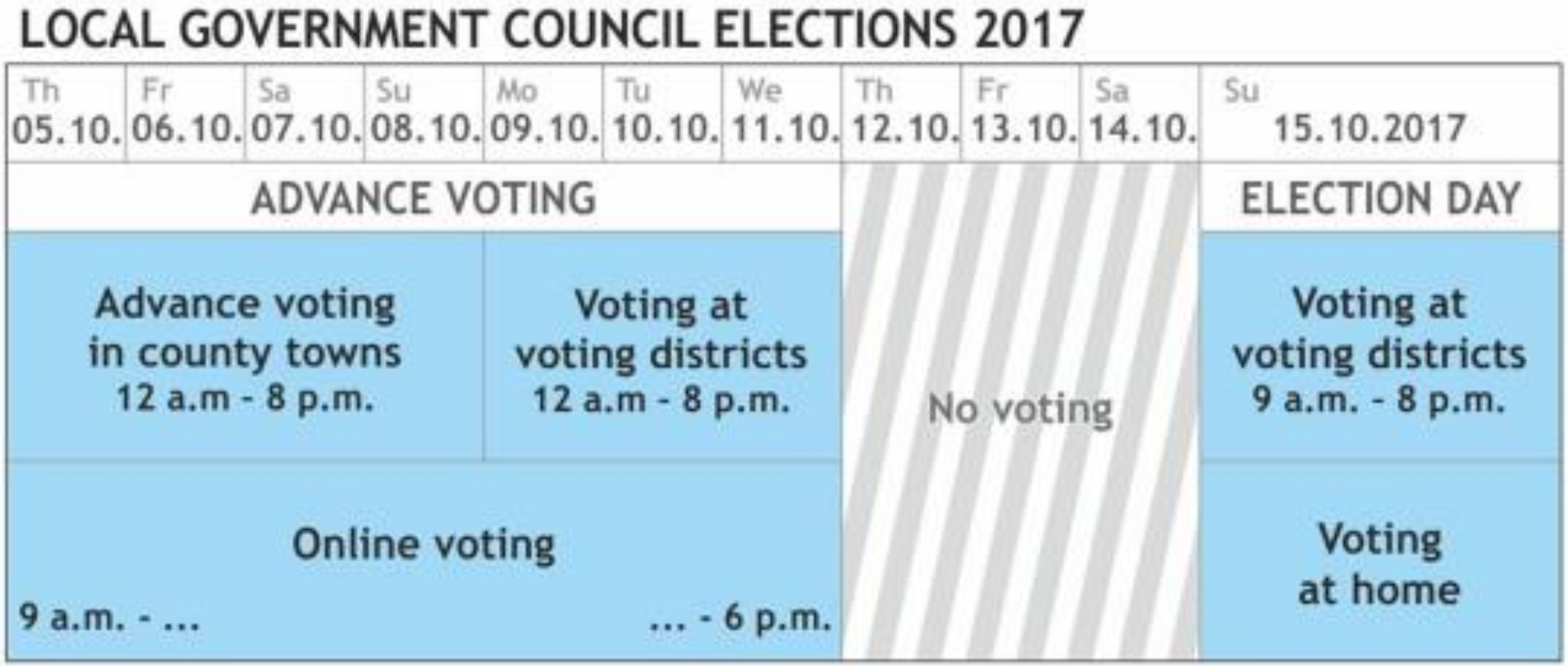
The spread of internet voting



Ingredients

- Widely used eID
  - Estonia: ID-card 2002, Mobile-ID 2007
  - 2020: over 1 billion digital signatures given
- Electronic voters registry
- Political will
- E-voting system

Voting in Estonia



LOCAL GOVERNMENT COUNCIL ELECTIONS 2017

Th 05.10.	Fr 06.10.	Sa 07.10.	Su 08.10.	Mo 09.10.	Tu 10.10.	We 11.10.	Th 12.10.	Fr 13.10.	Sa 14.10.	Su 15.10.2017
ADVANCE VOTING							No voting			ELECTION DAY
Advance voting in county towns 12 a.m - 8 p.m.				Voting at voting districts 12 a.m - 8 p.m.						Voting at voting districts 9 a.m. - 8 p.m.
Online voting 9 a.m. - ...						... - 6 p.m.				Voting at home

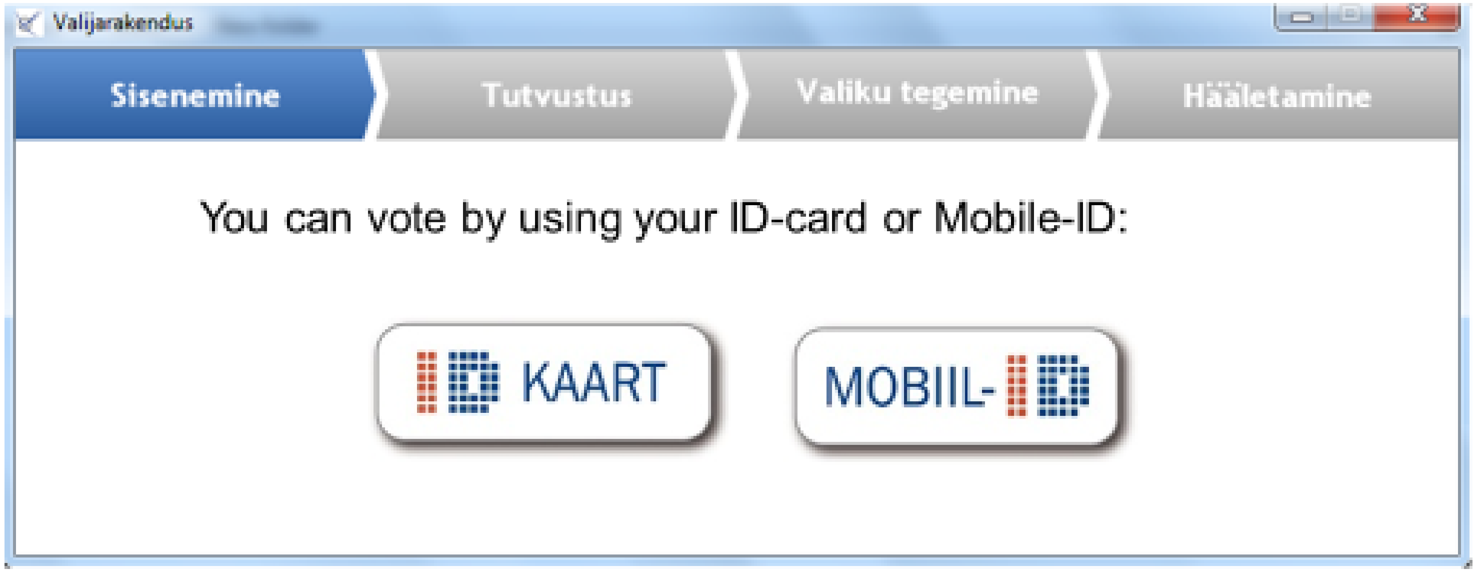
User authentication: ID-card or Mobile-ID

- ID-card (PIN 1,2)
- ID-card reader
- PC with ID-card reader
- Internet
- ID-card software

- Mobile-ID SIM card (PIN 1,2)
- Mobile phone (works on any handset)
  - or PC/tablet & mobile phone
- Mobile network coverage
- **No special software**

Run the Application

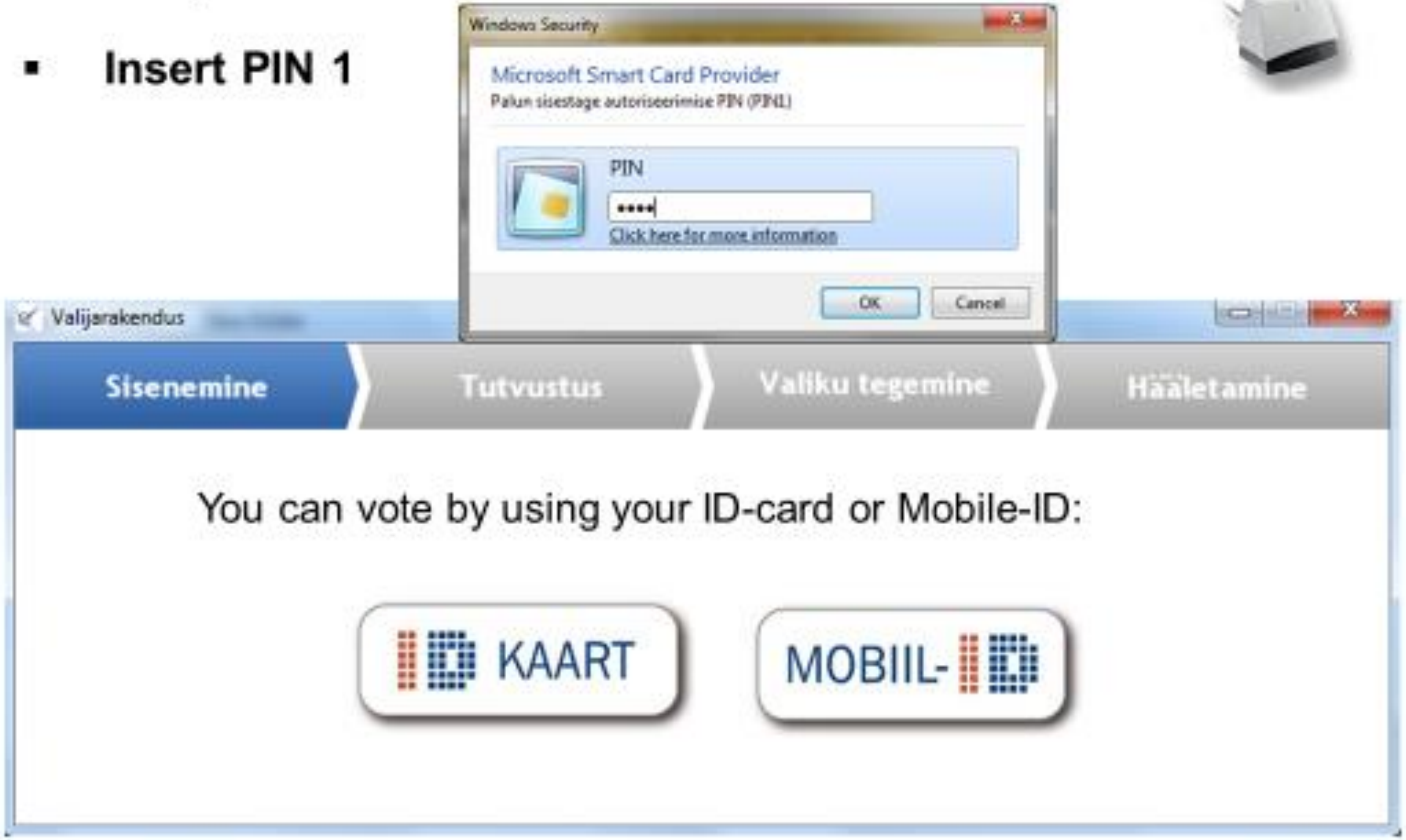
- Select your eID



You can vote by using your ID-card or Mobile-ID:

In case of ID-card... ****

- Put your card into card reader
- Insert PIN 1



Windows Security

Microsoft Smart Card Provider

Palun sisestage autoriseerimise PIN (PIN1)

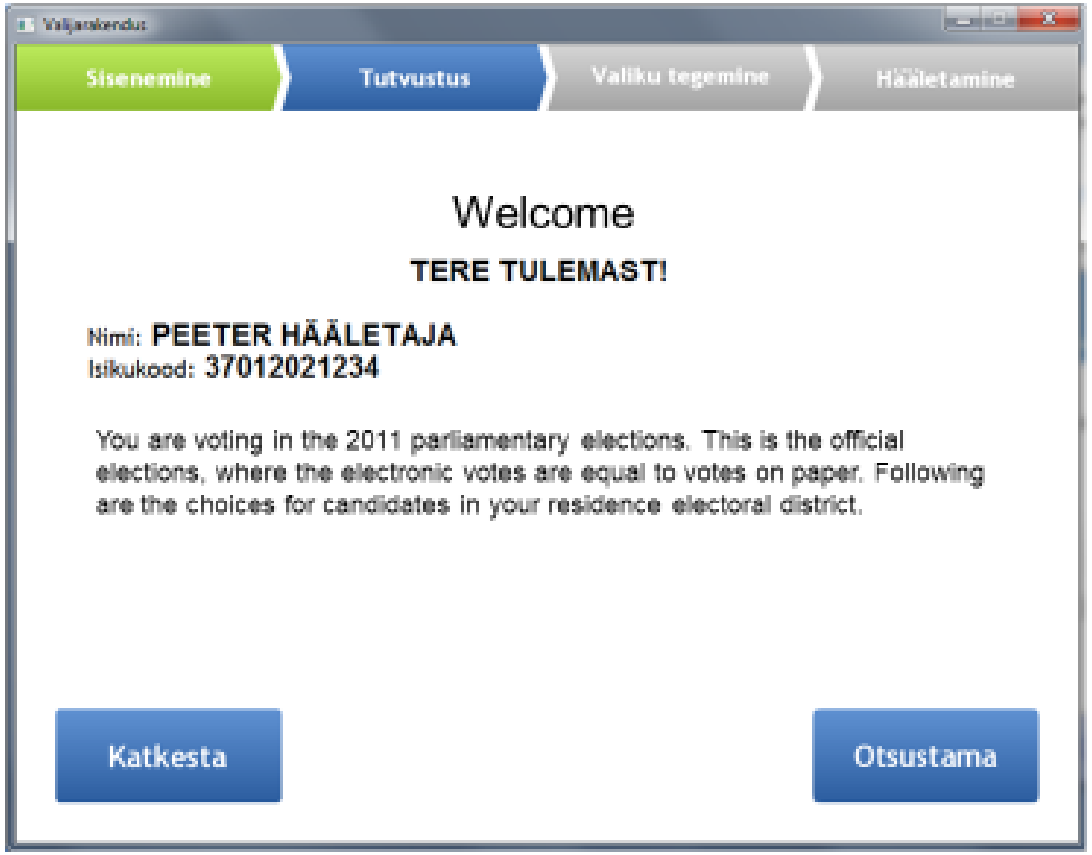
PIN: ****

Click here for more information

Valijarakendus

You can vote by using your ID-card or Mobile-ID:

You are identified



Welcome

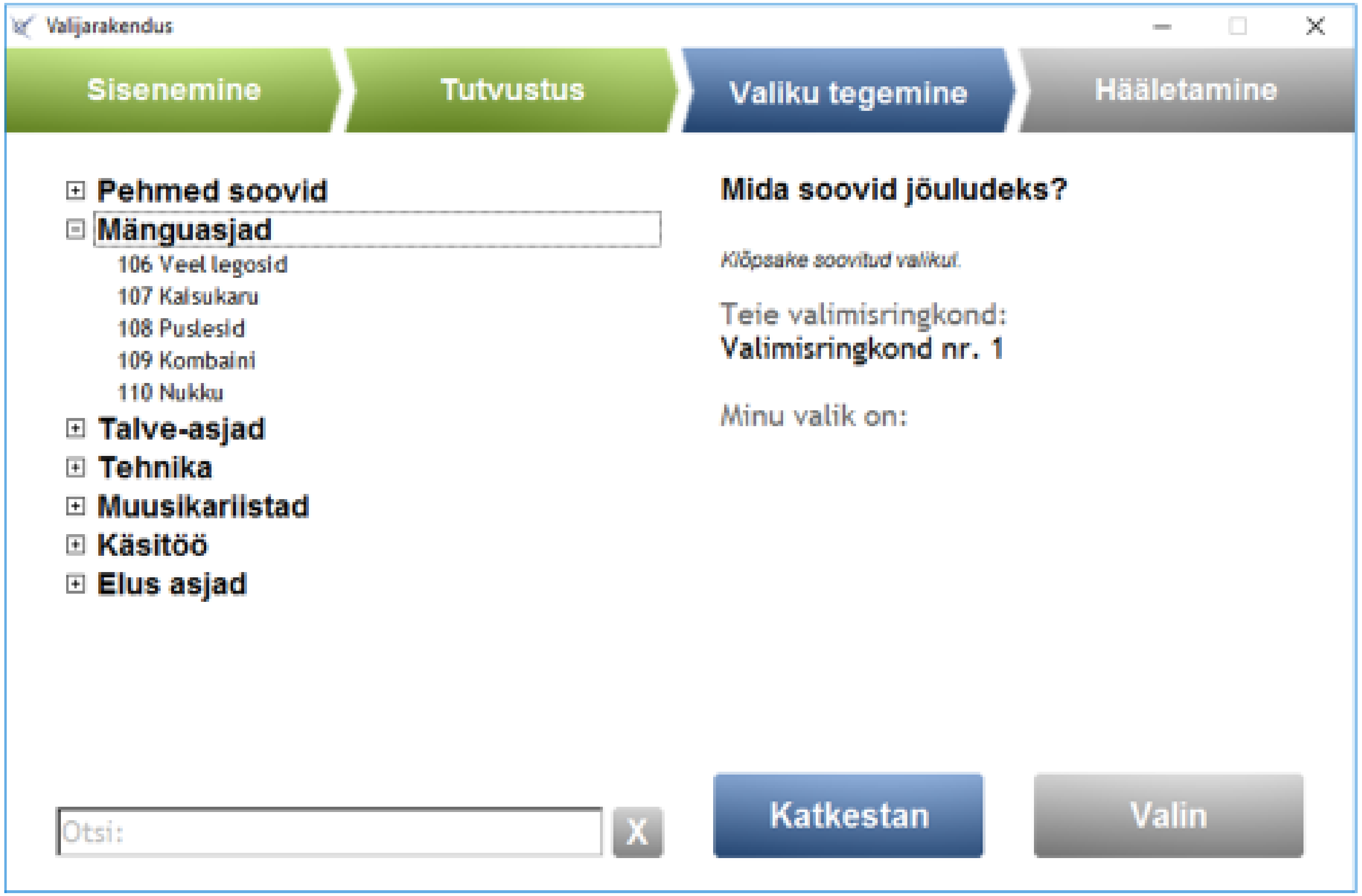
TERE TULEMAST!

Nimi: PEETER HÄÄLETAJA
Isikukood: 37012021234

You are voting in the 2011 parliamentary elections. This is the official elections, where the electronic votes are equal to votes on paper. Following are the choices for candidates in your residence electoral district.

Ballot completion

- Choose a candidate



⊞ Pehmed soovid

⊟ Mänguasjad

106 Veel legosid
107 Kaisukaru
108 Puslesid
109 Kombaini
110 Nukku

⊞ Talve-asjad

⊞ Tehnika

⊞ Muusikariistad

⊞ Käsitöö

⊞ Elus asjad

Mida soovid jõuludeks?

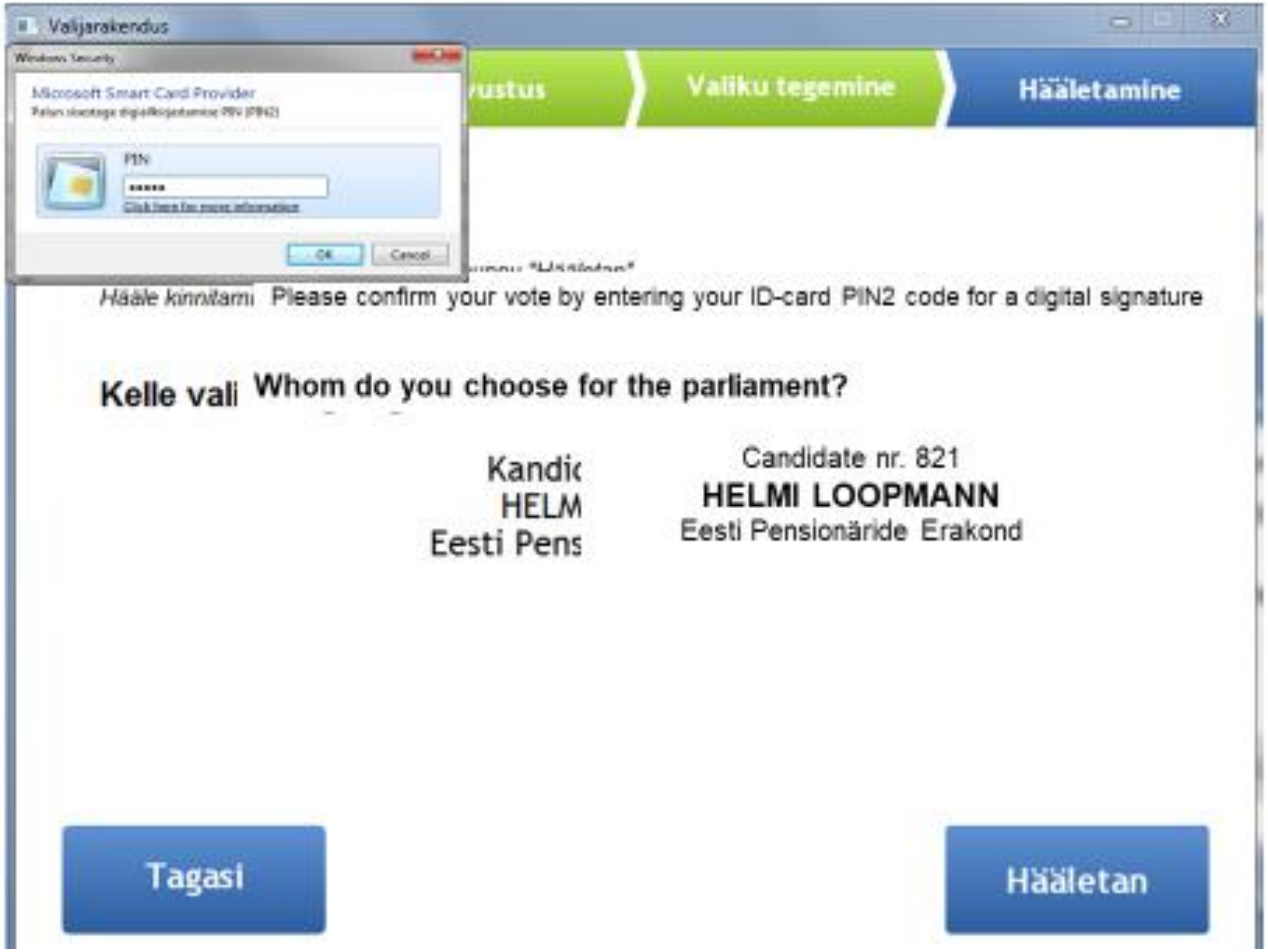
Klõpsake soovitud valikul.

Teie valimisringkond:
Valimisringkond nr. 1

Minu valik on:

Confirmation (ID-card)

- **Confirm your choice with PIN2**



Microsoft Smart Card Provider

Palun sisestage digiallkirjastamise PIN (PIN2)

PIN: *****

Click here for more information

Hääle kinnitami Please confirm your vote by entering your ID-card PIN2 code for a digital signature

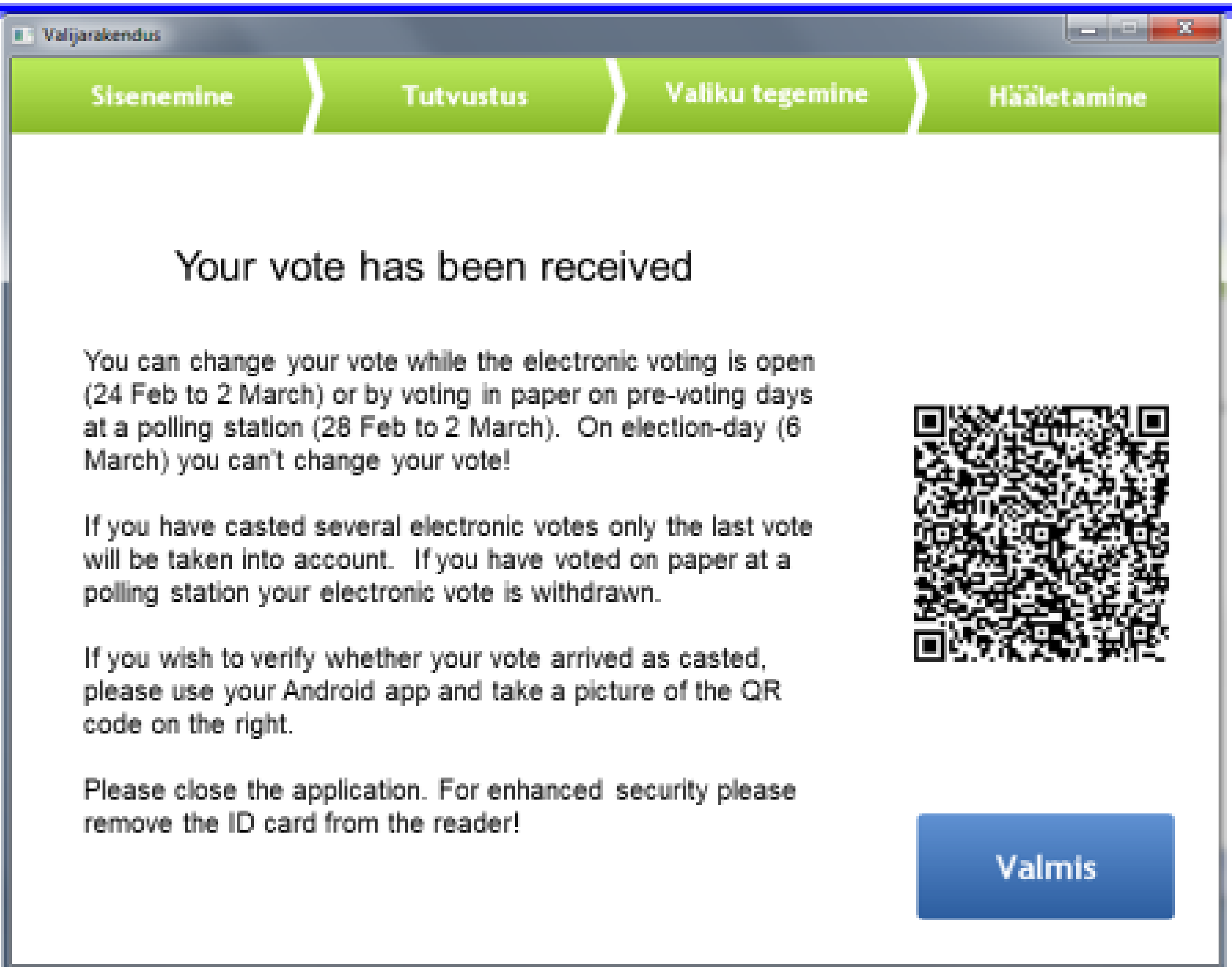
Kelle vali Whom do you choose for the parliament?

Kandic Candidate nr. 821

HELM HELMI LOOPMANN

Eesti Pens Eesti Pensionäride Erakond

Vote received



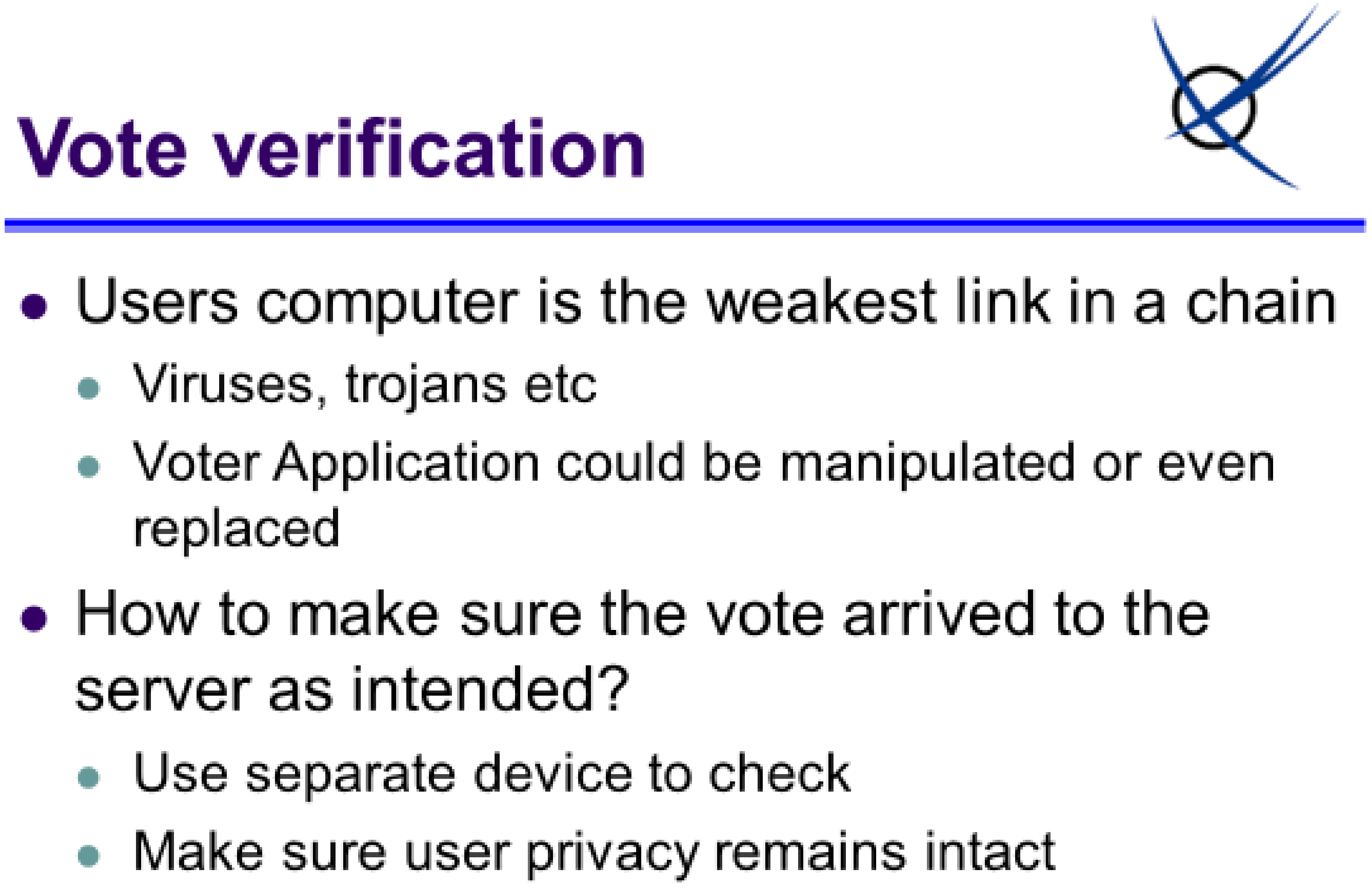
Your vote has been received

You can change your vote while the electronic voting is open (24 Feb to 2 March) or by voting in paper on pre-voting days at a polling station (28 Feb to 2 March). On election-day (6 March) you can't change your vote!

If you have casted several electronic votes only the last vote will be taken into account. If you have voted on paper at a polling station your electronic vote is withdrawn.

If you wish to verify whether your vote arrived as casted, please use your Android app and take a picture of the QR code on the right.

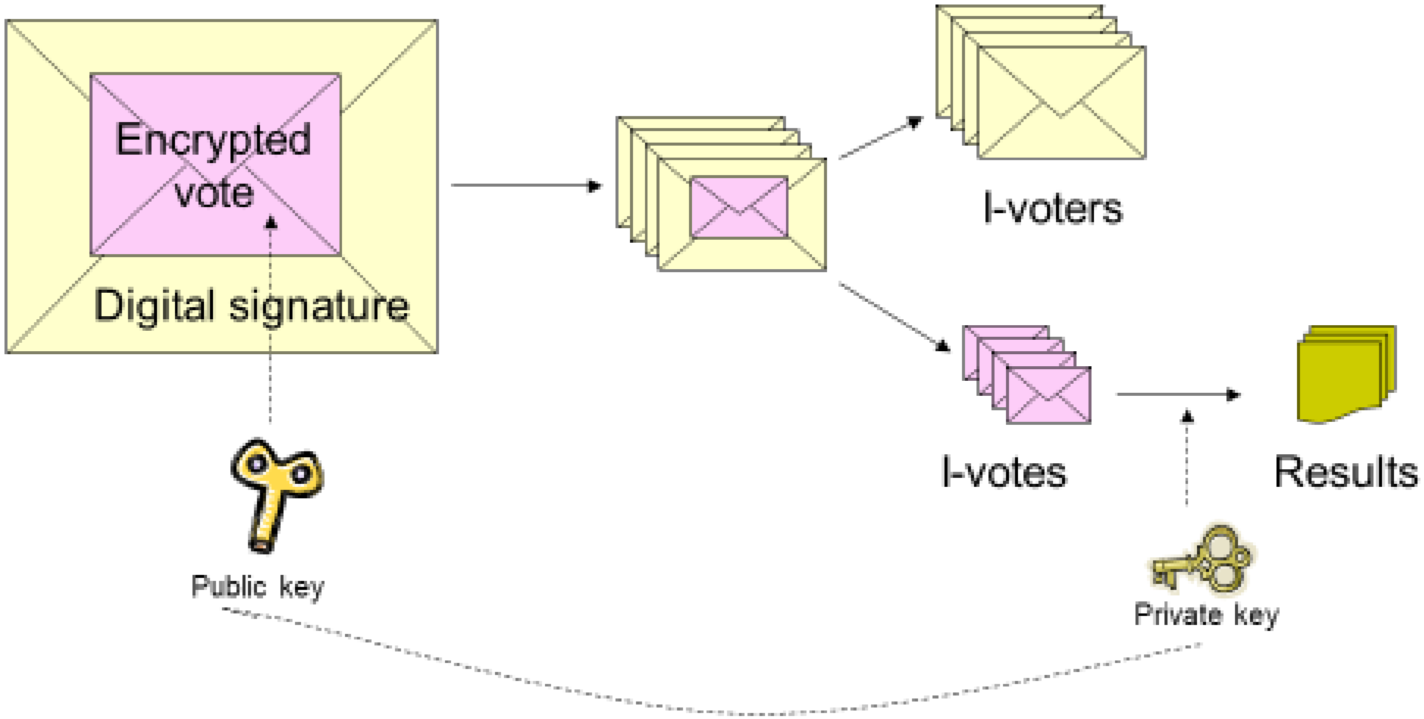
Please close the application. For enhanced security please remove the ID card from the reader!



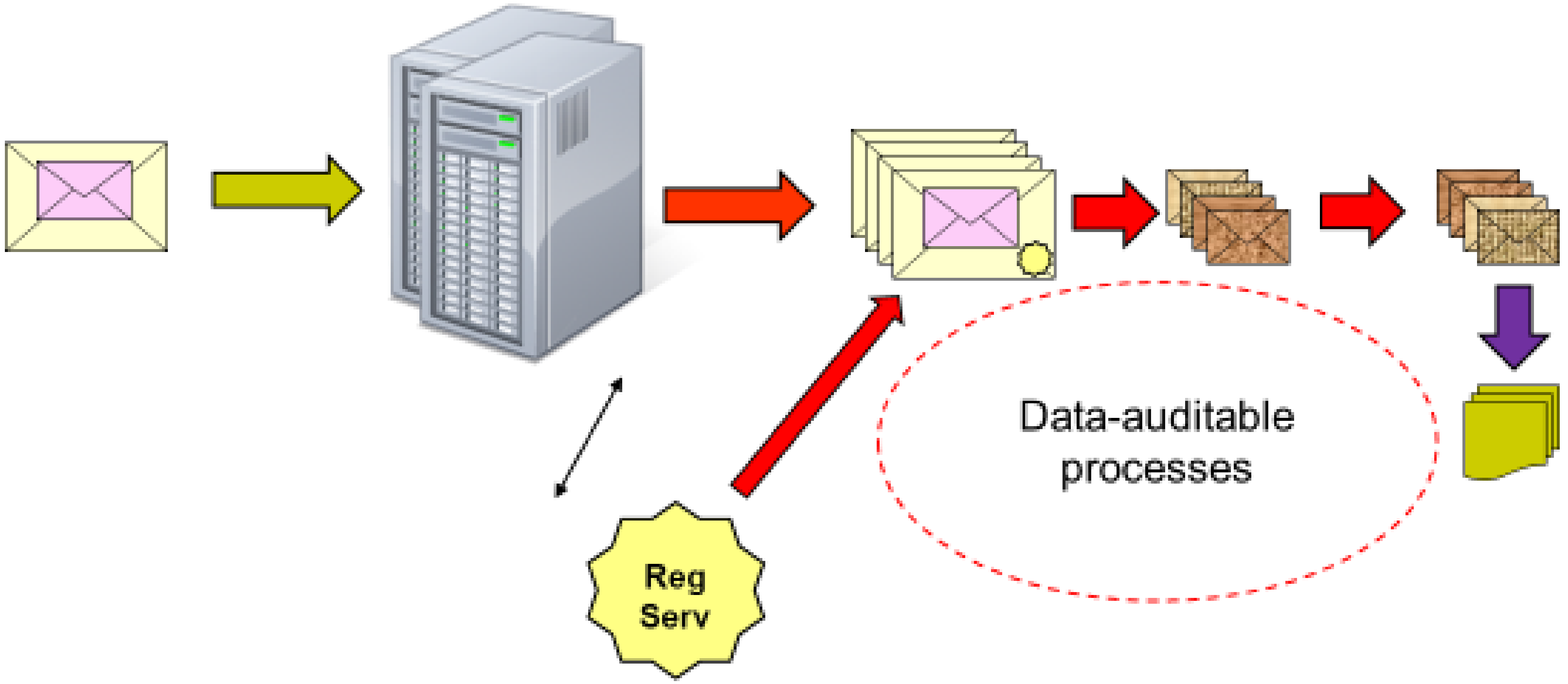
Vote verification

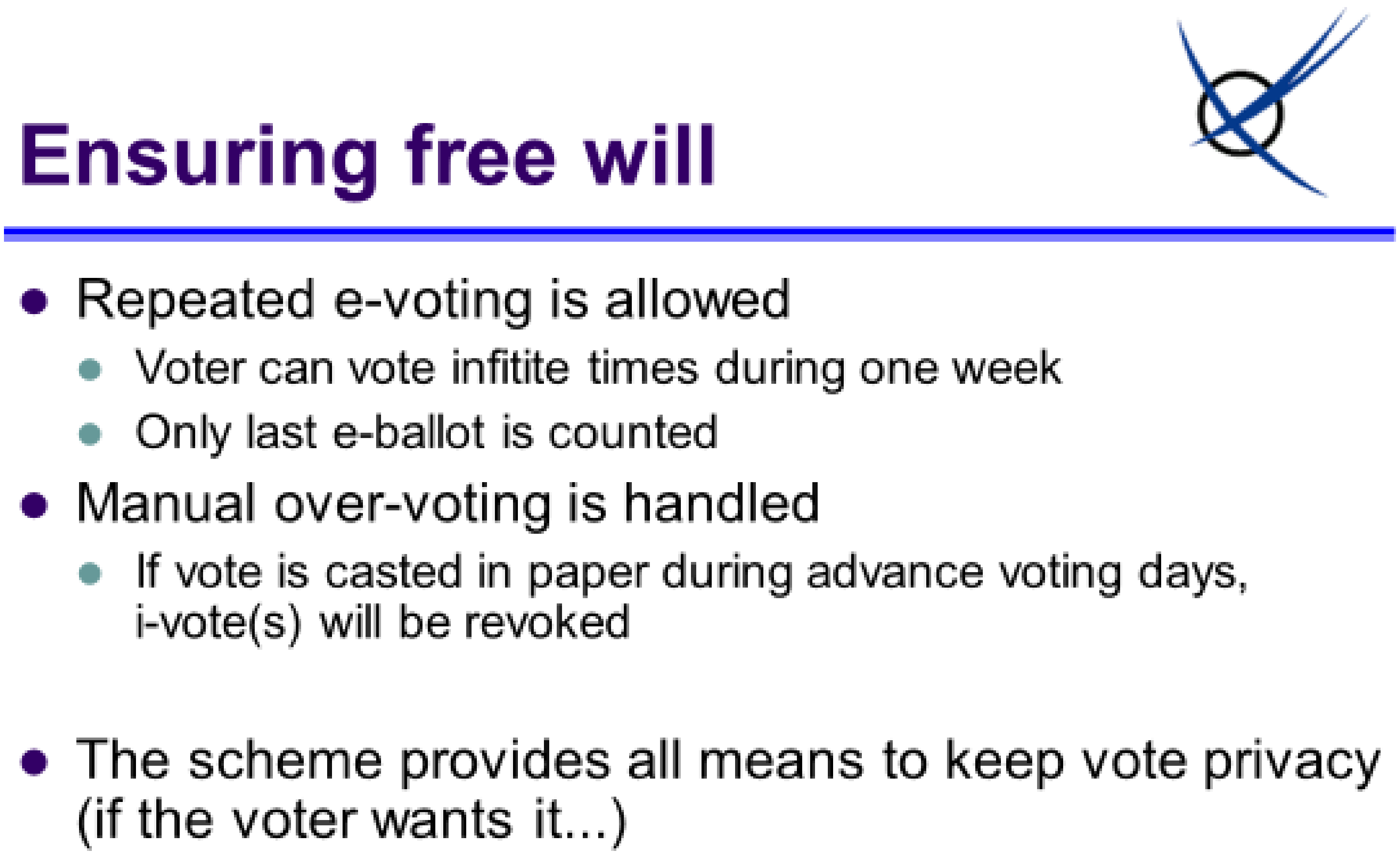
- Users computer is the weakest link in a chain
  - Viruses, trojans etc
  - Voter Application could be manipulated or even replaced
- How to make sure the vote arrived to the server as intended?
  - Use separate device to check
  - Make sure user privacy remains intact

Envelope scheme



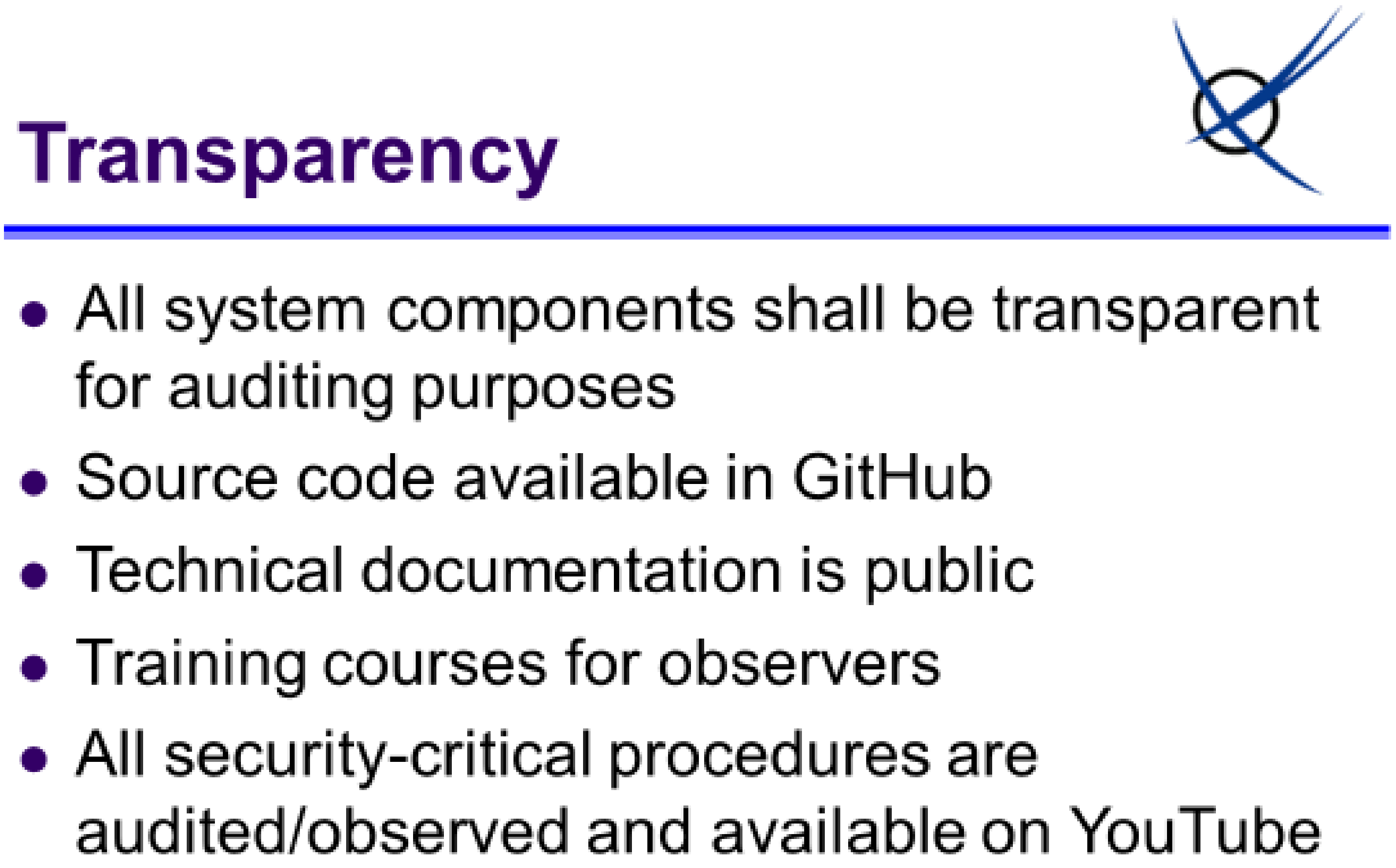
Ensuring end-to-end security





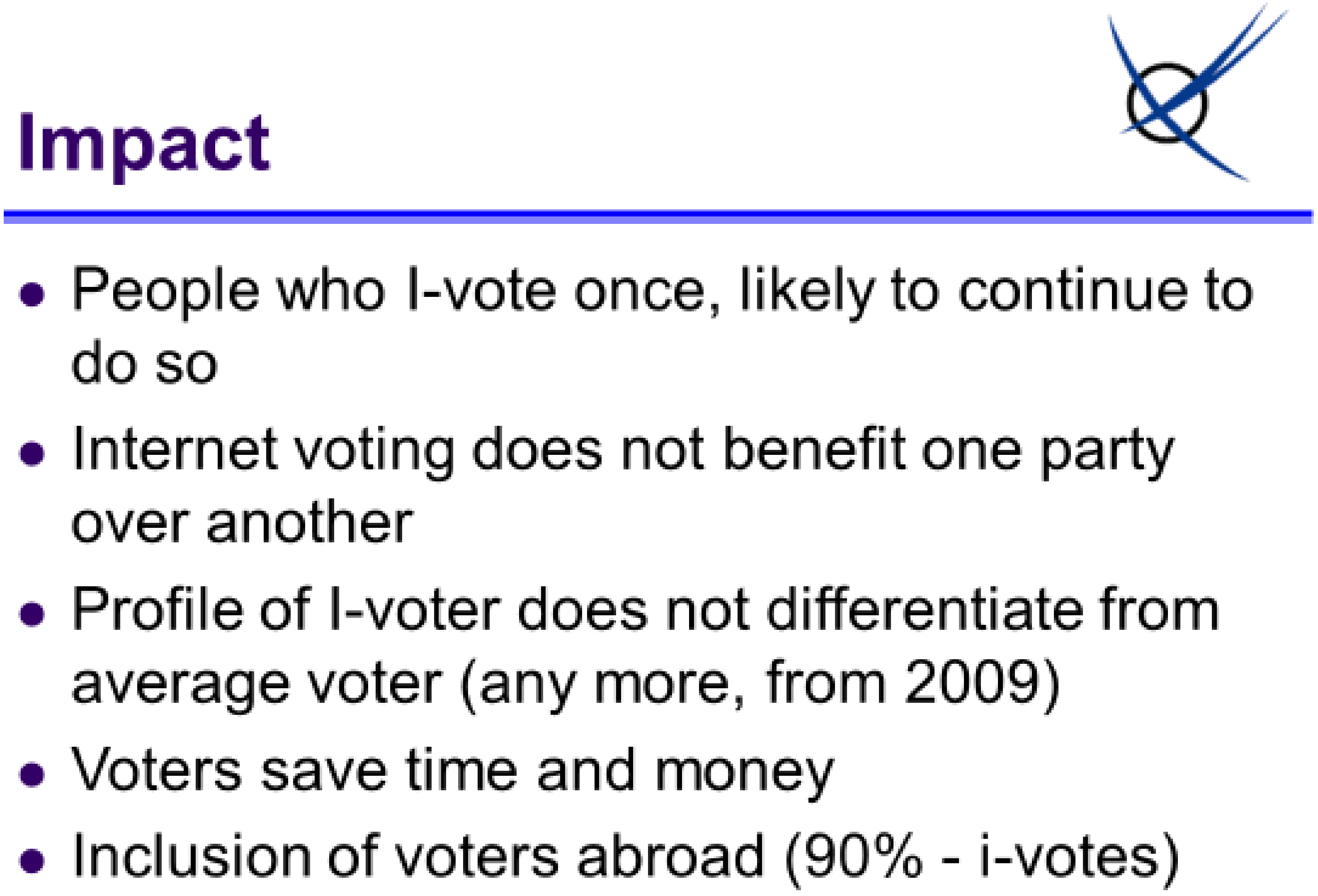
Ensuring free will

- Repeated e-voting is allowed
  - Voter can vote infitite times during one week
  - Only last e-ballot is counted
- Manual over-voting is handled
  - If vote is casted in paper during advance voting days, i-vote(s) will be revoked
- The scheme provides all means to keep vote privacy (if the voter wants it...)



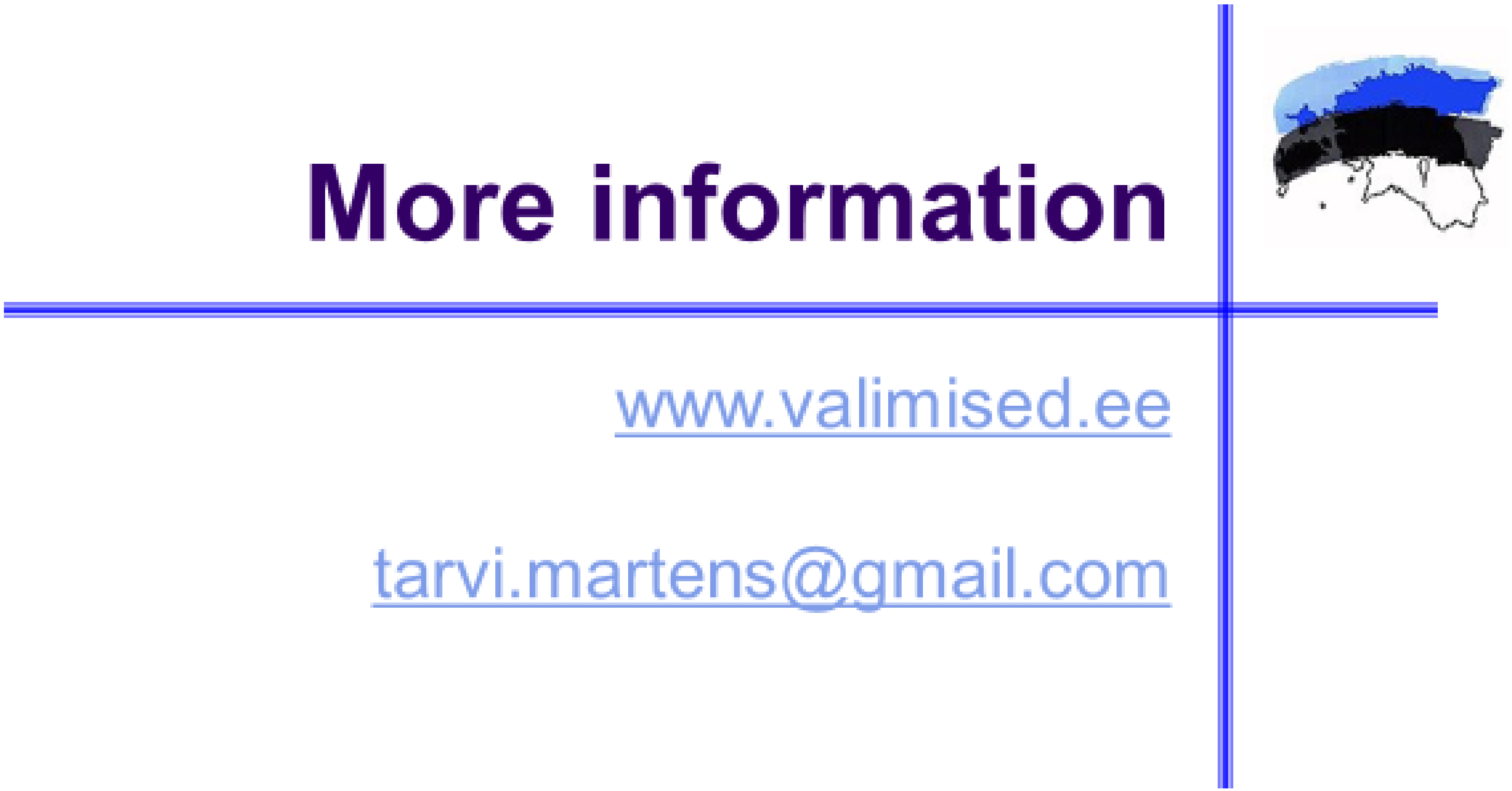
Transparency

- All system components shall be transparent for auditing purposes
- Source code available in GitHub
- Technical documentation is public
- Training courses for observers
- All security-critical procedures are audited/observed and available on YouTube



Impact

- People who I-vote once, likely to continue to do so
- Internet voting does not benefit one party over another
- Profile of I-voter does not differentiate from average voter (any more, from 2009)
- Voters save time and money
- Inclusion of voters abroad (90% - i-votes)



More information

www.valimised.ee

tarvi.martens@gmail.com