ELECTIONS
DIGITAL TECHNOLOGIES
HUMAN RIGHTS

Council of Europe
documents

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

ELECTIONS
DIGITAL TECHNOLOGIES
HUMAN RIGHTS

Council of Europe documents

Council of Europe

This compendium was developed by the Division of Division of Elections and Civil Society of the Council of Europe within the framework of the Council of Europe project on "Supporting the transparency, inclusiveness and integrity of electoral practice in Ukraine". The compendium is aimed at increasing public awareness about standards and policies of the Council of Europe in the respective field.
The documents collected herein are not necessarily comprehensive, complete, accurate or up to date. The compendium is developed only for information purposes. For professional or legal advice, please, consult a suitably qualified professional.

Cover photo, design and layout:
Kateryna Kysla

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

Printed at the Council of Europe

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

ELECLAB

URSO
Useful
Relevant
Sustainable
Owned

Contents

Resolution 1459 (2005)[1]
of the Parliamentary Assembly of the Council of Europe

Abolition of restrictions on the right to vote

1. The Parliamentary Assembly, in line with its Recommendation 1500 (2001) on the participation of immigrants and foreign residents in political life in the Council of Europe member states, stresses the importance of the right to vote and to stand in elections as a basic precondition for preserving other fundamental civil and political rights upheld by the Council of Europe. Electoral rights are the basis of democratic legitimacy and representativeness of the political process. They should, therefore, evolve to follow the progress of modern societies towards ever inclusive democracy.

2. In accordance with the opinion of the European Commission for Democracy through Law (Venice Commission) adopted in December 2004, it therefore invites the member and observer states of the Organisation to reconsider all existing restrictions to electoral rights and to abolish all those that are no longer necessary and proportionate in pursuit of a legitimate aim.

3. The Assembly considers that, as a rule, priority should be given to granting effective, free and equal electoral rights to the highest possible number of citizens, without regard to their ethnic origin, health, status as members of the military or criminal record. Due regard should be given to the voting rights of citizens living abroad.

4. In line with the case-law of the European Court of Human Rights, any exceptions to this rule must be prescribed by law, pursue a legitimate aim and not be arbitrary or disproportionate.

1. Assembly debate on 24 June 2005 (24th Sitting) (see Doc. 10553, report of the Committee on Legal Affairs and Human Rights, rapporteur: Mr Eker; and Doc. 10577, opinion of the Political Affairs Committee, rapporteur: Lord John Tomlinson). Text adopted by the Assembly on 24 June 2005 (24th Sitting).

Source: www.assembly.coe.int

5. All legal residents are normally obliged to pay local taxes and their lives are directly affected by the decisions of local authorities. The right to vote and to stand as candidates in local elections should therefore be granted to all legal residents having lived long enough in the country, regardless of their nationality or ethnic origin. In this context, the Assembly urges the countries concerned to implement the recommendations by the Council of Europe Commissioner for Human Rights on granting that right to residents with the special status of "non-citizens", in accordance with the Convention on the Participation of Foreigners in Public Life at Local Level (ETS No. 144).

6. In view of the possible conflict of loyalties between the country of which a person is a national and the country of residence, the right to vote and stand as a candidate in national elections (parliamentary or presidential) should generally be attached to nationality. Persons having several nationalities should be allowed to choose freely in which country they wish to exercise their right to vote.

7. Given the importance of the right to vote in a democratic society, the member countries of the Council of Europe should enable their citizens living abroad to vote during national elections bearing in mind the complexity of different electoral systems. They should take appropriate measures to facilitate the exercise of such voting rights as much as possible, in particular by considering absentee (postal), consular or e-voting, consistent with Recommendation Rec(2004)11 of the Committee of Ministers to member states on legal, operational and technical standards for e-voting. Member states should co-operate with one another for this purpose and refrain from placing unnecessary obstacles in the path of the effective exercise of the voting rights of foreign nationals residing on their territories.

8. Considering that rehabilitation of prisoners, aimed at their reintegration into society – giving them all the rights and duties accorded to other citizens – is one of the purposes of criminal sanctions, the Assembly regrets that in many countries persons convicted of a criminal offence are barred from voting, in some cases even for some time after their release from prison. A more modern approach would be to limit the withdrawal of the right to vote to crimes committed against the democratic process (for example, election fraud, illicit pressure on voters or candidates, participation in a military putsch, participation in terrorist activities as established by a court judgment). In any case, in view of the judgment of the European Court of Human Rights in the case of Hirst v. the United Kingdom (30 June 2004), national parliaments should reconsider existing restrictions and determine whether they still pursue a legitimate aim and are not arbitrary or disproportionate.

9. As stressed by the Venice Commission, the need for democratic control over the military should not be used as an excuse to automatically deprive military servicemen of their voting rights.

10. The Assembly also stresses the importance of protecting the voting rights of vulnerable groups, such as residents of nursing homes, prison inmates, soldiers and handicapped people. Appropriate measures must be taken to avoid

any undue influence by helpers, supervisors or hierarchical superiors, in particular by ensuring the secrecy of the vote.

11. The Assembly therefore invites:

the Council of Europe member and observer states concerned to:

- *a. reduce minimum age requirements for active and passive electoral rights to 18 years for the right to vote and 25 years for the right to stand as candidates;*
- *b. grant electoral rights to all their citizens (nationals), without imposing residency requirements;*
- *c. facilitate the exercise of expatriates' electoral rights by providing for absentee voting procedures (postal and/or consular voting) and considering the introduction of e-voting consistent with Recommendation Rec(2004)11 of the Committee of Ministers and to co-operate with one another to this end;*
- *d. to sign and ratify the 1992 Council of Europe Convention on the Participation of Foreigners in Public Life at Local Level and to grant active and passive electoral rights in local elections to all legal residents;*
- *e. to reconsider existing restrictions on the electoral rights of prisoners, persons who have been convicted of a criminal offence and members of the military, with a view to abolishing all those that are no longer necessary and proportionate in pursuit of a legitimate aim;*
- *f. to take appropriate measures to protect the electoral rights of vulnerable groups of voters (in particular, persons living in nursing homes, prisoners, members of the military, nomadic groups), in line with the Venice Commission's Code of Good Practice in Electoral Matters adopted in July 2003;*

the Council of Europe, and in particular the Venice Commission, to develop further its activities aimed at improving the conditions for the effective exercise of electoral rights, putting a special emphasis on co-operation aimed at facilitating the exercise of electoral rights by expatriate citizens.

Resolution 1970 (2014)[1]
of the Parliamentary Assembly of the Council of Europe

Internet and politics: the impact of new information and communication technology on democracy

1. The Parliamentary Assembly notes that the expansion of the Internet has had major consequences in terms of the exercise of the fundamental rights which are central to the construction of our democratic societies, such as the right to freedom of information, expression, opinion, assembly and association, and the protection of an individual's privacy.

2. This expansion and the exponential acceleration of the capacity for transmission on the network have put an end to the concentration of informative power and changed the paradigm of communication. The public space has been enlarged and the web has become an enormous unbounded field, a veritable global forum where all individuals can seek and exchange information, share knowledge, express opinions on any subject and become committed to an idea or a cause.

3. The upheavals caused by the Internet have altered the relationship between the political world and citizens and the balance between representative democracy and direct democracy. They make it imperative for us to discuss both the new prospects that are opening up for a stronger and more dynamic form of democracy and the new dangers which may undermine it, along with the role that legislators should play in this process.

4. The Internet helps citizens to rally together and ensures increased visibility for their action. It has also radically changed institutional communication and the

1. Assembly debate on 29 January 2014 (5th Sitting) (see Doc. 13386, report of the Committee on Culture, Science, Education and Media, rapporteur: Ms Anne Brasseur; and Doc. 13399, opinion of the Committee on Political Affairs and Democracy, rapporteur: Mr Hans Franken). Text adopted by the Assembly on 29 January 2014 (5th Sitting). See also Recommendation 2033 (2014).
Source: www.assembly.coe.int

structure of the relationship between voters and the political parties, as well as among citizens, elected representatives and government departments. More broadly, it has extended the possibilities for participation in political life. The Internet is thus an essential part of modern democracy, and the political institutions must take account of the plethora of citizen participation initiatives which take shape on the web.

5. The development of communication technologies in future will allow the use of electronic voting for the expansion of the traditional mechanisms of democracy. This process should be gradual.

6. However, the Assembly does not think that in today's complex world it would be possible to replace the universal-suffrage model of political representation with any sort of model based primarily on processes of direct democracy through electronic channels, even supposing that everyone had access to the consultation procedures and voted via the Internet and that appropriate means were found to remove all obstacles to the general use of electronic voting.

7. The definition and implementation of policies necessitate a number of long-term choices, requiring complex negotiations and involving conflicting interests which are difficult to balance; such complexity is not sufficiently appreciated in the decision-making processes on the web, which must necessarily simplify the content of discussions. Public policies also require internal coherency and co-ordination, to which the fragmentation of the decision-making process on the web would set up insuperable obstacles.

8. Lastly, in such a system, those people – having more resources and necessarily fewer in number – who would ***de facto*** dictate the final decisions would neither be known nor required to account for these decisions, and would therefore wield a type of power which was both illegitimate and unaccountable. In this case we can no longer speak of democracy.

9. Participation and representation are inseparable; this requires representative democracy to be genuinely participative. For several years now, the Assembly has been regularly observing the erosion of public confidence in political institutions. In order to halt this tendency, politicians should listen more, develop citizen participation and promote active citizenship.

10. In this regard, the Assembly notes that the Internet and social media are opening new doors to enlarged dialogue between citizens and elected representatives and stimulating more dynamic participation in democratic life. We must seize this opportunity to reconnect the democratic institutions, via the Internet, with the citizens who have moved away from them, and develop, particularly in our parliaments, the capacities and competences required for exploiting this positive potential provided by the Internet.

11. Alongside the elected representatives, the political parties have an extremely important role to play; the Assembly invites them to reflect on their relations with their electoral bases and on the use of new information and communication technology in order to develop permanent dialogue with voters and involve them in devising, and subsequently implementing, their political programmes.

12. However, the Assembly is aware that the Internet increases the risks of abuses and aberrations liable to jeopardise human rights, the rule of law and democracy: it accommodates the expression of intolerance, hatred and violence against children and women; it fuels organised crime, international terrorism and dictatorships; it also intensifies the risk of biased information and manipulation of opinion, and facilitates insidious monitoring of our private lives.

13. Control over the lawful use of data processed on the web is difficult: national legislations on data protection differ and privacy policies of the transnational Internet corporations – which are the world's largest personal data operators – are subject only to the law of the States where the corporations are registered. It is especially worrying that personal data have been reduced to tradeable goods and are misused for commercial or political purposes, posing a serious threat to the protection of private lives. In addition, the increased use of new semantic polling techniques can lead to the manipulation of public opinion and distort political processes.

14. The Internet belongs to everyone; therefore, it belongs to no one and has no borders. We must preserve its openness and neutrality. However, the Internet must not be allowed to become a gigantic prying mechanism, operating beyond all democratic control. We must prevent the web from becoming a ***de facto*** no-go area, a sphere dominated by hidden powers in which no responsibility can be clearly assigned to anyone.

15. The accountability of Internet operators is therefore a key issue which the Assembly is currently dealing with via two reports on the right to Internet access and on co-ordinated strategies for effective Internet governance. At the European Union level, the "Code of EU online rights" and the "Digital Agenda for Europe" initiatives are also concerned with this issue.

16. Web surfers can help make the Internet a safer environment which respects human rights and the operators must shoulder their responsibilities in fighting abuses and aberrations. Self-regulation is vital here to guarantee Internet neutrality and should be encouraged; it would not, however, appear to be sufficient.

17. States must take concerted action and adopt common rules, while ensuring that the supervisory mechanisms themselves do not threaten fundamental freedoms, to protect the Internet as an area of freedom. The revelations about the operations of intelligence agencies which go beyond any legal framework by ordering systematic intrusions into private life are unacceptable; this must lead us to reflect seriously on the price we pay for our security and on the precautions which we must take in order to avoid annihilating the space for freedom on the Internet.

18. National parliaments provide key forums for discussing democracy and the possible renewal of the democratic system in the Internet age; they must, however, open up, intensively involve all stakeholders – such as state institutions, private entities and commercial companies – and mobilise the whole of civil society for the debate on democracy, politics and the Internet.

19. Accordingly, the Assembly recommends that the member States, and in particular their national parliaments:

- 19.1. increase the capacity of the political – and in particular the parliamentary – institutions to use new information and communication technology to improve the transparency of the decision-making process and dialogue with citizens, in particular through social networks, parliamentary Internet channels and other platforms allowing citizens to provide feedback;
- 19.2. continue, in this context, developing targeted Internet training programmes for elected representatives, modernising the websites of parliaments and governments and improving the use of online consultation and participation facilities;
- 19.3. not merely reproduce traditional tools online but reach out to citizens in the virtual spaces they are creating and think creatively about the Internet's potential as a platform for engagement and knowledge sharing;
- 19.4. use the Internet more effectively as a source of aggregate data that can be used to identify citizens' preferences and needs so that the political agenda on all levels of government better reflects the issues of concern to society, while bearing in mind the long-term effects in the context of the general interest;
- 19.5. take advantage of the functions of the Internet to boost co-operation between the authorities, civil society and universities with a view to developing and implementing initiatives to promote political and democratic engagement among citizens;
- 19.6. combat the socio-cultural inequalities which perpetuate the digital divide, including by introducing educational programmes aimed at teenagers and young students so that they acquire the necessary competences for using the Internet as well-informed web surfers;
- 19.7. promote the convergence of education in the new media and education for democratic citizenship and human rights, which should take due account of the advantages and problems of the Internet, and develop programmes capable of reaching the various age brackets and social groups; these programmes should mobilise school and university circles, social partners and the media;
- 19.8. invite universities to develop academic courses in the area of data science, including ethical, technical, legal, economic and societal aspects;
- 19.9. initiate, both at the national level and within the Council of Europe, discussions on norms and mechanisms, keeping pace with the development of the technologies, required for:
    - 19.9.1. creating a safe space on the web while also guaranteeing freedom of expression as set out in Article 10 of the European

Convention on Human Rights (ETS No. 5) and the protection of private life as set out in Article 8;

- 19.9.2. preventing the risk of information distortion and manipulation of public opinion, and consider, for instance:
- 19.9.2.1. devising coherent regulations and/or incentives for self-regulation concerning the accountability of the major Internet operators;
- 19.9.2.2. establishing an independent institution with sufficient powers, technical competences and resources to give expert opinions on the algorithms of the search engines which filter and regulate access to information and knowledge on the web, while averting the risk that such an institution could undermine the very nature of freedom of expression;
- 19.9.2.3. developing principles and general standards for regulating the new semantic polling practices;
- 19.9.2.4. devising regulations that must be applied by companies offering Internet communication systems to prevent the abuse of individuals' personal or family life by trolling activities, while maintaining a balance with freedom of expression;

- 19.10. ensure on the one hand respect for human rights on the web and, on the other, freedom of the Internet, and take action within the international bodies responsible for Internet governance to preserve these rights and this freedom throughout the world, especially where democracy has been weakened, threatened or abolished;
- 19.11. unreservedly support the proposal to launch the preparation of a Council of Europe white paper on democracy, politics and the Internet set out by the Assembly in its Recommendation 2033 (2014) "Internet and politics: the impact of new information and communication technology on democracy".
- 19.12. pursue the reflection, in close co-operation with the European Commission for Democracy through Law (Venice Commission), with a view to elaborating a protocol to the European Convention on Human Rights on the right to participate in the conduct of public affairs, as stressed in Resolution 1746(2010) and Recommendation 1928 (2010) "Democracy in Europe: crisis and perspectives", and pay special attention to the role of the Internet and other digital tools of participation, such as social networks, online discussion platforms, electronic voting and open government initiatives.

Recommendation CM/Rec(2017)5[1]

of the Committee of Ministers of the Council of Europe to member States on standards for e-voting

Adopted by the Committee of Ministers of the Council of Europe on 14 June 2017 at the 1289th meeting of the Ministers' Deputies

PREAMBLE

The Committee of Ministers, under the terms of Article 15.b of the Statute of the Council of Europe,

Considering that the aim of the Council of Europe is to achieve a greater unity between its members for the purpose of safeguarding and promoting the ideals and principles which are their common heritage;

Reaffirming its belief that representative and direct democracy is part of that common heritage and is the basis of the participation of citizens in political life at the level of the European Union and at national, regional and local levels;

Having regard to the obligations and commitments as undertaken within existing international instruments and documents, such as:

- the Universal Declaration on Human Rights;
- the International Covenant on Civil and Political Rights;
- the United Nations Convention on the Elimination of All Forms of Racial Discrimination;
- the United Nations Convention on the Elimination of All Forms of Discrimination against Women;

1. When adopting this recommendation, the Permanent Representative of the Russian Federation indicated that, in accordance with Article 10.2c of the Rules of Procedure for the meetings of the Ministers' Deputies, he reserved the right of his government to comply or not with the recommendation.

Source: www.coe.int/cm

- the United Nations Convention on the Rights of Persons with Disabilities;
- the United Nations Convention against Corruption;
- the Convention for the Protection of Human Rights and Fundamental Freedoms (ETS No. 5), in particular the Protocol thereto (ETS No. 9);
- the European Charter of Local Self-Government (ETS No. 122);
- the Convention on Cybercrime (ETS No. 185);
- the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (ETS No. 108);
- the Additional Protocol to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows (ETS No. 181);
- the Convention on the Standards of Democratic Elections, Electoral Rights and Freedoms in the Member States of the Commonwealth of Independent States (CDL-EL(2006)031rev);
- Recommendation Rec(99)5 of the Committee of Ministers to member States on the protection of privacy on the Internet;
- Recommendation Rec(2004)15 of the Committee of Ministers to member States on electronic governance (e-governance);
- Recommendation CM/Rec(2009)1 of the Committee of Ministers to member States on electronic democracy (e-democracy);
- the document of the Copenhagen Meeting of the Conference on the Human Dimension of the OSCE;
- the Charter of Fundamental Rights of the European Union;
- the Code of Good Practice in Electoral Matters, adopted by the Council for Democratic Elections of the Council of Europe and the European Commission for Democracy through Law (Venice Commission) and supported by the Committee of Ministers, the Parliamentary Assembly and the Congress of Local and Regional Authorities of the Council of Europe;

Bearing in mind that the right to vote lies at the foundations of democracy, and that, consequently, all voting channels, including e-voting, shall comply with the principles of democratic elections and referendums;

Recognising that the use of information and communication technologies by member States in elections has increased considerably in recent years;

Noting that some member States already use, or are considering using e-voting for a number of purposes, including:

- enabling voters to cast their votes from a place other than the polling station in their voting district;

- facilitating the casting of the vote by the voter;
- facilitating the participation in elections and referendums of citizens entitled to vote and residing or staying abroad;
- widening access to the voting process for voters with disabilities or those having other difficulties in being physically present at a polling station and using the devices available there;
- increasing voter turnout by providing additional voting channels;
- bringing voting in line with new developments in society and the increasing use of new technologies as a medium for communication and civic engagement in pursuit of democracy;
- reducing, over time, the overall cost to the electoral authorities of conducting an election or referendum;
- delivering voting results reliably and more quickly;
- providing the electorate with a better service, by offering a variety of voting channels;

Valuing the experience gathered by the member States that have used e-voting in recent years and of the lessons learned through such experience;

Aware also of the experience resulting from the application of Recommendation Rec(2004)11 of the Committee of Ministers to member States on legal, operational and technical standards for e-voting, the Guidelines for developing processes that confirm compliance with prescribed requirements and standards (Certification of e-voting systems) and the Guidelines on transparency of e-enabled elections;

Reaffirming its belief that public trust in the authorities in charge of managing elections is a precondition to the introduction of e-voting;

Aware of concerns about potential security, reliability or transparency problems of e-voting systems;

Conscious, therefore, that only those e-voting systems which are secure, reliable, efficient, technically robust, open to independent verification and easily accessible to voters will build public confidence, which is a prerequisite for holding e-elections;

Aware of the need for the member States to take into account the environment in which e-voting is implemented;

Aware that, in the light of recent technical and legal developments on e-enabled elections in Council of Europe member States, the provisions of Recommendation Rec(2004)11 need to be thoroughly revised and brought up to date;

Having regard to the work of the Ad hoc Committee of Experts on Legal, Operational and Technical Standards for e-voting (CAHVE), set up by the Committee of Ministers with the task of updating Recommendation Rec(2004)11,

1. Recommends that the governments of member States when introducing, revising or updating, as the case may be, domestic legislation and practice in the field of e-voting:

   i. respect all the principles of democratic elections and referendums;

   ii. assess and counter risks by appropriate measures, in particular as regards those risks which are specific to the e-voting channel;

   iii. be guided in their legislation, policies and practice by the standards included in Appendix I to this recommendation. The interconnection between the above-mentioned standards and those included in the accompanying Guidelines on the implementation of this recommendation should be taken into account;

   iv. keep under review their policy on, and experience of, e-voting, and in particular how and to what extent the provisions of this recommendation are being implemented in order to provide the Council of Europe with a basis for holding review meetings on the implementation of this recommendation at least every two years following its adoption;

   v. share their experience in this field;

   vi. ensure that this recommendation, its accompanying Explanatory Memorandum and Guidelines are translated and disseminated as widely as possible, and more specifically among electoral management bodies, election officials, citizens, political parties, domestic and international observers, NGOs, media, academics, providers of e-voting solutions and e-voting specific controlling bodies;

2. Agrees to regularly update the provisions of the Guidelines accompanying this recommendation;

3. Repeals Recommendation Rec(2004)11 on legal, operational and technical standards for e-voting and the Guidelines thereto.

APPENDIX I – E-VOTING STANDARDS

I. Universal suffrage

1. The voter interface of an e-voting system shall be easy to understand and use by all voters.

2. The e-voting system shall be designed, as far as is practicable, to enable persons with disabilities and special needs to vote independently.

3. Unless channels of remote e-voting are universally accessible, they shall be only an additional and optional means of voting.

4. Before casting a vote using a remote e-voting system, voters' attention shall be explicitly drawn to the fact that the e-election in which they are submitting their decision by electronic means is a real election or referendum.

II. Equal suffrage

5. All official voting information shall be presented in an equal way, within and across voting channels.

6. Where electronic and non-electronic voting channels are used in the same election or referendum, there shall be a secure and reliable method to aggregate all votes and to calculate the result.

7. Unique identification of voters in a way that they can unmistakably be distinguished from other persons shall be ensured.

8. The e-voting system shall only grant a user access after authenticating her/him as a person with the right to vote.

9. The e-voting system shall ensure that only the appropriate number of votes per voter is cast, stored in the electronic ballot box and included in the election result.

III. Free suffrage

10. The voter's intention shall not be affected by the voting system, or by any undue influence.

11. It shall be ensured that the e-voting system presents an authentic ballot and authentic information to the voter.

12. The way in which voters are guided through the e-voting process shall not lead them to vote precipitately or without confirmation.

13. The e-voting system shall provide the voter with a means of participating in an election or referendum without the voter exercising a preference for any of the voting options.

14. The e-voting system shall advise the voter if he or she casts an invalid e-vote.

15. The voter shall be able to verify that his or her intention is accurately represented in the vote and that the sealed vote has entered the electronic ballot box without being altered. Any undue influence that has modified the vote shall be detectable.

16. The voter shall receive confirmation by the system that the vote has been cast successfully and that the whole voting procedure has been completed.

17. The e-voting system shall provide sound evidence that each authentic vote is accurately included in the respective election results. The evidence should be verifiable by means that are independent from the e-voting system.

18. The system shall provide sound evidence that only eligible voters' votes have been included in the respective final result. The evidence should be verifiable by means that are independent from the e-voting system.

IV. Secret suffrage

19. E-voting shall be organised in such a way as to ensure that the secrecy of the vote is respected at all stages of the voting procedure.

20. The e-voting system shall process and store, as long as necessary, only the personal data needed for the conduct of the e-election.

21. The e-voting system and any authorised party shall protect authentication data so that unauthorised parties cannot misuse, intercept, modify, or otherwise gain knowledge of this data.

22. Voters' registers stored in or communicated by the e-voting system shall be accessible only to authorised parties.

23. An e-voting system shall not provide the voter with proof of the content of the vote cast for use by third parties.

24. The e-voting system shall not allow the disclosure to anyone of the number of votes cast for any voting option until after the closure of the electronic ballot box. This information shall not be disclosed to the public until after the end of the voting period.

25. E-voting shall ensure that the secrecy of previous choices recorded and erased by the voter before issuing his or her final vote is respected.

26. The e-voting process, in particular the counting stage, shall be organised in such a way that it is not possible to reconstruct a link between the unsealed vote and the voter. Votes are, and remain, anonymous.

V. Regulatory and organisational requirements

27. Member States that introduce e-voting shall do so in a gradual and progressive manner.

28. Before introducing e-voting, member States shall introduce the required changes to the relevant legislation.

29. The relevant legislation shall regulate the responsibilities for the functioning of e-voting systems and ensure that the electoral management body has control over them.

30. Any observer shall be able to observe the count of the votes. The electoral management body shall be responsible for the counting process.

VI. Transparency and observation

31. Member States shall be transparent in all aspects of e-voting.

32. The public, in particular voters, shall be informed, well in advance of the start of voting, in clear and simple language, about:

- any steps a voter may have to take in order to participate and vote;
- the correct use and functioning of an e-voting system;
- the e-voting timetable, including all stages.

33. The components of the e-voting system shall be disclosed for verification and certification purposes.

34. Any observer, to the extent permitted by law, shall be enabled to observe and comment on the e-elections, including the compilation of the results.

35. Open standards shall be used to enable various technical components or services, possibly derived from a variety of sources, to interoperate.

VII. Accountability

36. Member States shall develop technical, evaluation and certification requirements and shall ascertain that they fully reflect the relevant legal and democratic principles. Member States shall keep the requirements up to date.

37. Before an e-voting system is introduced and at appropriate intervals thereafter, and in particular after any significant changes are made to the system, an independent and competent body shall evaluate the compliance of the e-voting system and of any information and communication technology (ICT) component with the technical requirements. This may take the form of formal certification or other appropriate control.

38. The certificate, or any other appropriate document issued, shall clearly identify the subject of evaluation and shall include safeguards to prevent its being secretly or inadvertently modified.

39. The e-voting system shall be auditable. The audit system shall be open and comprehensive, and actively report on potential issues and threats.

VIII. Reliability and security of the system

40. The electoral management body shall be responsible for the respect for and compliance with all requirements even in the case of failures and attacks. The electoral management body shall be responsible for the availability, reliability, usability and security of the e-voting system.

41. Only persons authorised by the electoral management body shall have access to the central infrastructure, the servers and the election data. Appointments of persons authorised to deal with e-voting shall be clearly regulated.

42. Before any e-election takes place, the electoral management body shall satisfy itself that the e-voting system is genuine and operates correctly.

43. A procedure shall be established for regularly installing updated versions and corrections of all relevant software.

44. If stored or communicated outside controlled environments, the votes shall be encrypted.

45. Votes and voter information shall be kept sealed until the counting process commences.

46. The electoral management body shall handle all cryptographic material securely.

47. Where incidents that could threaten the integrity of the system occur, those responsible for operating the equipment shall immediately inform the electoral management body.

48. The authenticity, availability and integrity of the voters' registers and lists of candidates shall be maintained. The source of the data shall be authenticated. Provisions on data protection shall be respected.

49. The e-voting system shall identify votes that are affected by an irregularity.

APPENDIX II – GLOSSARY OF TERMS

In this recommendation and Explanatory Memorandum, the following terms are used with the following meanings:

- access control: the prevention of unauthorised use of a resource;
- assessment: an evaluation of persons, hardware, software and procedures to verify if they are suitable for the fulfilment of certain tasks;
- audit: an independent pre- or post-election evaluation of a person, organisation, system, process, entity, project or product which includes quantitative and qualitative analysis;
- authentication: the provision of assurance of the claimed identity of a person or data;
- availability: the state of being accessible and usable upon demand;
- ballot: the legally recognised means by which the voter can express his or her vote;
- candidate: a voting option consisting of a person, a group of persons and/or a political party;
- casting of the vote: entering the vote in the ballot box;
- certificate: a document which is the result of a formal certification wherein a fact is certified or attested;
- certification: a process of confirmation that an e-voting system is in compliance with prescribed requirements and standards and that it includes, at the minimum, provisions to ascertain the correct functioning of the system. This can be done through measures ranging from testing and auditing through to formal certification. The end result is a report and/or a certificate;
- certification body (or certifier): an organisation entitled to conduct a certification process and to issue a certificate upon completion of the process;
- certification report: a document which explains what a certificate has certified and how it is certified;
- chain of trust: a process in computer security which is established by validating each component of hardware and software from the bottom up. It is

intended ensure that only trusted software and hardware can be used while still remaining flexible;

- component testing: a method by which individual units of the system code are tested to determine if they are fit for use;
- confidentiality: the state characterising information that should not be made available or disclosed to unauthorised individuals, entities or processes;
- controlled environment: premises supervised by election officials, e.g. polling stations, embassies or consulates;
- e-election: a political election or referendum where e-voting is used;
- electoral management body (EMB): institution in charge of managing elections in a given country at national or lower level;
- electronic ballot box: the electronic means by which the votes are stored pending being counted;
- e-vote: electronically cast vote;
- e-voting: the use of electronic means to cast and/or count the vote;
- e-voting system: the hardware, software and processes which allow voters to vote by electronic means in an election or referendum;
- formal certification: certification carried out by official authorities, only before election day and leading to the issuance of a certificate;
- guidelines: any document that aims to streamline particular processes according to a set routine. By definition, guidelines are not legally binding;
- non-disclosure agreement (NDA): a legal contract between two or more parties that outlines confidential material, knowledge, or information that the parties wish to share with one another for certain purposes, but wish to restrict access to by parties not bound by the contract;
- open access: access online to material that is free for all to read, and possibly to use (or reuse) within certain limits;
- protection profile: an implementation-independent set of security requirements for a category of products that meet the specific security needs of consumers;
- requirement: a singular documented need of what a particular product or service should be or perform;
- remote e-voting: the use of electronic means to cast the vote outside the premises where voting takes place in general;
- sealing: protecting information so that it cannot be used or interpreted without the help of other information or means available only to specific persons or authorities, including through encryption;

- to stakeholder: a person, group, organisation, or system that has an impact on, or can be affected by, a government's or organisation's actions. These include citizens, election officials, political parties, governments, domestic and international observers, media, academics, (I)NGOs, anti-e-voting organisations and specific e-voting certification bodies;
- standard (legal): refers to provisions contained in Appendix I to Recommendation CM/Rec(2017)5;
- standard (technical): an established norm usually in the form of a formal document that establishes uniform engineering or technical criteria, methods, processes and practices;
- testing: the process of verifying that the system works as expected;
- vote: the expression of the choice of voting option;
- voter: a person who is entitled to cast a vote in a particular election or referendum;
- voting channel: the way by which the voter can cast a vote;
- voting options: the range of possibilities from which a choice can be made through the casting of the vote in an election or referendum;
- voters' register: a list of persons entitled to vote (electors).

Explanatory Memorandum[1]

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

(Adopted by the Committee of Ministers of the Council of Europe on 14 June 2017 at the 1289th meeting of the Ministers' Deputies)

Ad hoc Committee of Experts on Legal, Operational and Technical Standards for e-voting (CAHVE)

(Item considered by the GR-DEM at its meetings on 20 April and 1 June 2017)

BACKGROUND

1. The present Recommendation on standards for e-voting and explanatory memorandum are the updated version of the "Recommendation Rec(2004)11 of the Committee of Ministers to member States on legal, operational and technical standards for e-voting" and its explanatory memorandum which were adopted on 30 September 2004. In 2010 two complementary documents were approved: the "Guidelines for developing processes that confirm compliance with prescribed requirements and standards in the region (Certification of e-voting systems)" and the "Guidelines on transparency of e-enabled elections".

2. The Recommendation Rec(2004)11 and the accompanying Guidelines have served as legal benchmarks to countries and institutions in the region when introducing, operating and evaluating e-voting systems. Following the conclusions of the 2012 and 2014 biannual review meetings of Rec(2004)11 and of an experts' meeting held in Vienna in December 2013, the Committee of Ministers decided on 1 April 2015, under Article 17 of the Statute of the Council of Europe and in accordance with Resolution CM/Res(2011)24 on intergovernmental committees and subordinate bodies, to set up an "Ad hoc committee of experts on legal, operational and technical standards for e-voting" (CAHVE).

3. CAHVE's mandate was to prepare a new Recommendation updating Rec(2004)11 and its explanatory memorandum in the light of recent technical and legal developments related to e-enabled elections in the Council of Europe member States. The update should consist in enhancing and further developing the

1. Source: www.coe.int/cm

existing Recommendation Rec(2004)11. Work should focus on redressing the identified flaws of the Recommendation, taking advantage of recent experiences with e-voting in the region and addressing the implications of emerging technical concepts and solutions. The updating process should be guided by a needs assessment, taking particular account of the views of member States and of non-governmental stakeholders. Based on its mandate CAHVE produced the following documents: Recommendation Rec(2017)XX on standards for e-voting revising and replacing Recommendation Rec(2004)11 on legal, operational and technical standards and the present explanatory memorandum. In addition to its mandate, CAHVE has prepared "Guidelines on the implementation of the provisions of Recommendation Rec(2017)XX on standards for e-voting".

4. The present Recommendation contains standards on e-voting which reflect and apply the principles of democratic elections and referendums to e-voting. Standards aim at guaranteeing the respect of the principles when using e-voting, thus building trust and confidence in domestic e-voting schemes.

5. Principles of democratic elections and referendums stem from existing Council of Europe and other international instruments in the field of elections. Standards express objectives that e-voting shall fulfil to conform to the principles of democratic elections and referendums. The standards are common to the Council of Europe region.

6. The competence of the member States of the Council of Europe in electoral matters and regarding referendums is not affected by this Recommendation. The Recommendation covers the use of e-voting in political elections and referendums. Political elections and referendums are held at different levels. In some countries no referendums are held. The standards apply in the same way whether e-voting is used in political elections or in political referendums.

7. The reasons for introducing or considering the introduction of e-voting differ from country to country and depend on the specific domestic context. It has become clear that an e-voting system can only be introduced if voters have trust and confidence in their electoral system and in election administration. The present Recommendation does not require member States to introduce e-voting. It observes that an increasing number of countries do currently make some use of e-voting or envisage to do so in the near future. The Recommendation introduces standards which aim at harmonizing the implementation of the principles of democratic elections and referendums when e-voting is used in member States.

8. In the present Recommendation, the term e-voting refers to the use of electronic means for voting and counting purposes, in controlled and uncontrolled environments. It covers e-voting machines in polling stations, the use of optical scanners to register and/or count paper ballots as well as remote e-voting. Unless specific mention, standards apply to all forms of e-voting. Standards which are specific only to one or to some forms do mention this. Detailed implementation provisions, often specific to one form of e-voting, are included

in the "Guidelines on the implementation of the provisions of Recommendation CM/Rec(2017)5 on standards for e-voting".

9. Electoral systems may include both non-remote and remote forms of voting. Remote voting can be conducted in both controlled (e.g. voting at embassies or consulates, voting at post offices or municipal offices) and uncontrolled (i.e. unsupervised by officials) environments (e.g. voting from home via postal mail or voting from a private computer via the internet). Each member State has its own established practice concerning the types of voting channels available to voters.[2] For the purpose of this Recommendation remote e-voting means the use of electronic means to cast the vote outside the premises where voting takes place in general.

10. The Recommendation addresses relevant aspects of e-voting relating to the different stages of elections and referendums, namely the pre-voting stage, the casting of the vote, and the post-voting stage, as well as to the roles and responsibilities of different stakeholders. The standards included here are applicable to the use of e-voting as defined in this Recommendation. Annex systems, which relate to e-voting but are not, technically speaking, part of it, such as voter registration systems for instance, require specific regulations. The present standards for e-voting may inspire such regulations. Member States contemplating the introduction of e-voting may also consider the Council of Europe e-voting Handbook "Key steps in the implementation of e-enabled elections" (2010), which provides assistance and guidance with this respect.

11. Detailed guidelines for the implementation of the objectives (expressed in the standards) are to be found in the new "Guidelines on the implementation of the provisions of Recommendation CM/Rec(2017)5 on standards for e-voting" that accompanies the present Recommendation. The new Guidelines include an updated version of the provisions of this level from the old Recommendation Rec(2004)11 and from the two Guidelines associated to it, namely the "Guidelines for developing processes that confirm compliance with prescribed requirements and standards in the region (Certification of e-voting systems)" and the "Guidelines on transparency of e-enabled elections". The new Guidelines replace both previous Guidelines.

12. The present version of the Guidelines needs to be completed through further work to address all forms and all aspects of e-voting covered by CM/Rec(2017)5 on standards for e-voting. Furthermore, due to ongoing developments in the legal and technical fields, the provisions included in the Guidelines need to be updated on a regular basis whereas the Recommendation is intended to provide a stable framework. The update of the Guidelines shall be considered and decided by member States at the periodic review meetings on the implementation of the present Recommendation.

2. The European Commission for Democracy through Law (Venice Commission) has provided a Report on the compatibility of remote voting and electronic voting with the requirements of the documents of the Council of Europe (Adopted by the Venice Commission at its 58th Plenary Session (Venice, 12-13 March 2004. Study no. 260, 2003, Strasbourg, 18 March 2004, CDL-AD (2004)012 Or. Fr.). The conclusion by the Venice Commission is that remote voting is compatible with the Council of Europe's standards, provided that certain preventative measures are observed in the procedures for either postal voting or electronic voting.

RECOMMENDATIONS

13. Democracy is inconceivable without elections and referendums held in accordance with certain principles that lend them their democratic status. These principles represent a specific aspect of the "European constitutional heritage" also known as the "European electoral heritage". In 2002, the European Commission for Democracy through Law (Venice Commission) adopted the Code of Good Practice in Electoral Matters[3] which, albeit non-binding, is the reference document of the Council of Europe in the field, and defines the "European Electoral Heritage" through two aspects: the hard core constitutional principles of electoral law and certain basic conditions necessary for their application. The Code identifies the following principles: universal, equal, free, secret and direct suffrage and periodically held elections. The basic conditions are: rule of law, respect for fundamental rights, stability of electoral law and effective procedural guarantees.[4] All voting channels used in elections and referendums, including e-voting, must be designed and implemented in conformity with these principles and conditions.

14. In line with the 2002 Code of Good Practice in Electoral Matters, the meaning of the principles and conditions can be summarised as follows:

- ***Universal suffrage:*** all human beings have the right to vote and to stand for election subject to certain conditions, such as age or nationality;
- ***Equal suffrage:*** each voter has the same number of votes, each vote has the same weight and equality of opportunity has to be ensured;
- ***Free suffrage:*** the voter has the right to form and to express his/her opinion in a free manner, without any coercion or undue influence;
- ***Secret suffrage:*** the voter has the right to vote secretly as an individual, and the state has the duty to protect that right;
- ***Direct suffrage:*** the ballots cast by the voters directly determine the person(s) elected;
- ***Frequency of elections:*** elections must be held at regular intervals;

3. Code of good practice in electoral matters (CDL-AD(2002)023rev), endorsed by Parliamentary Assembly resolution 1320(2003) and CLRAE Resolution 148 (2003), subject of a Declaration by the Committee of Ministers (114th session, 13 May 2004).

4. - Point 7 of the Document of the Copenhagen Meeting of the Conference on the Human Dimension of the OSCE of 29 June 1990 clearly speaks of free, universal, equal and secret suffrage - point 6 of direct suffrage, albeit in a qualified form

- Article 25(b) of the International Covenant on Civil and Political Rights expressly provides for all these principles except direct suffrage, although the latter is implied (Article 21 of the Universal Declaration of Human Rights).

- Article 3 of the Additional Protocol to the European Convention on Human Rights explicitly provides for the right to periodic elections by free and secret suffrage; the other principles have also been recognized in human rights case law (Universality: ECHR No. 9267 or81, judgment in Mathieu-Mohin and Clerfayt vs. Belgium, 2 March 1997, Series A vol. 113, p. 23; judgment in Gitonas and others vs. Greece, 1 July 1997, No. 18747 or91, 19376 or92; 19379 or92, 28208 or95 and 27755 or95, Collected Judgments and Decisions, 1997-IV, p. 1233; re. Equality: Aforementioned judgment in Mathieu-Mohin and Clerfayt, p. 23.) The right to direct elections has been admitted by the Strasbourg Court implicitly (ECHR No. 24833 or94, judgment in Matthews vs. The United Kingdom, 18 February 1999, Collected Judgments and Decisions 1999-I, para. 64.)

- ***Respect for fundamental rights:*** democratic elections require respect for human rights, such as freedom of expression, freedom of circulation, freedom of assembly, freedom of association;
- ***Regulatory levels and stability of electoral law:*** rules of electoral law must have at least the rank of a statute; rules on technical matters and detail may be included in regulations of the executive. The fundamental elements of electoral law should not be open to amendment less than one year before an election, or should be written in the constitution or at a level higher than ordinary law;
- ***Procedural guarantees:*** these include procedural safeguards aiming at ensuring the organisation of elections by an impartial body, the observation of elections by national and international observers, an effective system of appeal among others;
- ***Electoral system:*** within the respect of the above-mentioned principles, any electoral system may be chosen.

15. The standards included in the Appendix I to this Recommendation set objectives that e-voting shall fulfil to comply with the principles and conditions of the "European electoral heritage". However, not all the mentioned principles and conditions call for special attention and the setting of e-voting specific objectives. This is the case for instance with "periodically held elections" which does not require special attention when designing or implementing e-voting, if it's not for the obvious requirement that voting channels, including e-voting, should be ready to allow periodical elections to be held. The standards in this Recommendation address only those matters that were considered of specific relevance to e-voting.

Point I: recommendations I to vi

Recommendation i and ii: Respect of the principles and risk policy

16. E-voting, as any other voting method, must respect the principles for democratic elections and referendums. The rapid changes in its underlying technology present a challenge to such conformity as they introduce new opportunities and threats in an on-going manner. These must be managed appropriately. At the end, it is essential that the principles are not undermined by the introduction of electronically backed solutions in vote casting and/or counting proce-dures or by their evolution.

17. Accordingly, e-voting systems must be designed and operated in order to ensure constantly that the principles are respected. Member States should dedicate special attention to the risks inherent to the e-voting method chosen. E-voting specific risks need to be monitored permanently and appropriate countermeasures introduced whenever necessary. Given the rapid pace of change in the field of new technologies, member States are advised to introduce a risk management policy framework.

18. There may be exceptions to the principles; restrictions to the conditions for implementing the principles may apply. Furthermore, in an e-voting context, it may be necessary to have a stricter application of one principle and a looser application of another. These decisions are taken by the competent national authority (the Parliament, the supreme judge, the electoral management body or a governmental agency) and depend on the country's specific context. It is important that such decisions are taken in conformity with basic requirements such as being taken by the competent authority, having a basis in law, being of general interest, respecting proportionality, among others. The overall aim of democratic elections and referendums must be respected.

19. The principles for democratic elections to which the Recommendation refers are those of the European Electoral Heritage included in the Code of Good Practice in Electoral Matters of Venice Commission. They represent minimum requirements and apply throughout the region. A country may introduce additional principles or have a stricter interpretation of the principles included here. In such a case the e-voting will have to comply with principles and standards which are stricter than those of the present Recommendation.

Recommendation iii: Guidance by the Recommendation in reviewing domestic legislation, interconnection between Appendix I and the Guidelines

20. Respect for the principles is ensured in different ways and with different means depending on the voting channel and underlying technology. The standards included in Appendix I to the Recommendation translate the principles into concrete objectives. Guidance on how to implement the objectives is offered in the Guidelines. It is foreseen that the Guidelines will be completed and updated in the future on a regular basis so that they keep pace with practical experiences and the development of new technologies.

21. There exists a close relationship between the new Recommendation and the new Guidelines. Appendix I to the Recommendation contains high-level, hard core standards which express objectives that an e-voting system shall fulfil to respect the principles for democratic elections. Standards should be stable over time. Detailed provisions on how to implement the objectives (standards) are included in the Guidelines. They are based on experiences and developments in member States and on suggestions from academic research.

22. The Recommendation recommends member States, when introducing e-voting, to be guided in their relevant domestic legislation in the light of its provisions. Careful thought needs to be given to aspects of law other than those relating simply to the electronic equipment needed and its use. The extent of the review advisable will depend upon the existing laws of the member State in question. Examples include provisions specific to voting methods, criminal legislation relating to elections matters, data protection legislation or legislation on election observation.

23. Member States are recommended to take into consideration other modifications in legislation that may become necessary as a result of the introduction of e-voting.

Recommendations iv and v: Review of implementation and updating policy on the basis of shared experiences in the field

24. E-voting is a new and rapidly developing area. Standards and implementation guidelines need to keep abreast of legal and technical developments. In recognition of this, it is recommended that each member State keeps its own developments on e-voting under review, reports to the Council of Europe the results of such reviews and participates in the updating work of the Recommendation and of the Guidelines (see Point II). The Council will review the implementation of the Recommendation at least every two years after its adoption and the member States will share overall experiences in this field.

Recommendation vi: Translation and dissemination

25. The Recommendation and its accompanying Guidelines should be translated and disseminated by each member State in local language in order to inform the electoral management bodies, election officials, citizens, political parties, domestic and international observers, NGOs, media, academics, providers of e-voting solutions and e-voting specific controlling bodies adequately.

Point II: Update of the Guidelines

26. The Guidelines on the implementation of the provisions of Recommendation CM/Rec(2017)5 on standards for e-voting are a living document and should be up-dated regularly if legal, operational or technical developments make it necessary. The abovementioned review (para 24) would provide for an opportunity to assess such need.

Point III: Repealing of Rec(2004)11

27. The new CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting and the Guidelines on the implementation of the provisions of Recommendation CM/Rec(2017)5 shall repeal and replace the existing Recommendation Rec(2004)11 of the Committee of Ministers to member States on legal, operational and technical standards for e-voting and the "Guidelines for developing processes that confirm compliance with prescribed requirements and standards in the region (Certification of e-voting systems)" as well as the "Guidelines on transparency of e-enabled elections". This will avoid that any confusion subsist as to what principles, standards or Guidelines are henceforth applicable to e-voting in Council of Europe member States.

STANDARDS

28. The Appendix I to the Recommendation contains a set of standards on e-voting which express objectives that e-voting must fulfil to conform to the principles of democratic elections and referendums. They represent minimum standards, which, if followed in an e-voting system, would facilitate compliance with the principles of democratic elections and referendums. However, compliance with these standards alone does not guarantee the democratic quality of the e-election or e-referendum. National legislation may contain additional

requirements. The e-election or e-referendum has to be judged as a whole and in detail, in the specific context. But compliance with the standards is an important element in enhancing the democratic quality of the e-voting system.

INTERPRETATIVE DEFINITIONS

29. Appendix II at the end of the document contains definitions of terms used throughout the Recommendation, its Appendix I and the present Explanatory Memorandum. The definitions should also be consulted when the Recommendation or parts of it are translated into other languages.

APPENDIX I: E-VOTING STANDARDS

UNIVERSAL SUFFRAGE

Standard No. 1. "The voter interface of an e-voting system..."

30. In order to respect universal suffrage, member States need to ensure that the voter interface of the e-voting system is understandable and useable by as many voters as possible. Ergonomics need to be considered when designing an e-voting interface to take account of the interaction between the interface and the voter. The aim is that the voter can use the system easily and is able to execute the instructions, including the security-related ones.

31. Consideration must be given to different user-related constraints linked to age, language, lifestyle, etc. Instructions provided to voters shall be clear, easy to understand and to follow by as many voters as possible.

Standard No. 2. "The e-voting systems shall be designed..."

32. Not all persons with disabilities may be able to use e-voting. The design of the e-voting system should, however, aim to maximise the potential of accessibility that this voting channel provides for them. In conjunction with other voting channels available, e-voting aims at enabling as many persons with disabilities and special needs as possible to vote independently.

33. At the implementation level, the responsible authority decides how to accommodate the needs of people with disabilities and special needs. For example, individuals with a visual impairment or with dyslexia may need screen reading devices, sharply contrasting text and backgrounds, as well as the possibility of adjusting the text size in their Web browsers or on voting machines. Users with communication impairments may prefer graphically presented information. Those with co-ordination impairments may prefer using a keyboard rather than a mouse. Voting interfaces need to be adapted to the needs of mobility impaired users.

34. User-friendly solutions for the disabled may be less resistant to e-voting security threats. This is the reason why it's up to the responsible authority to decide to develop and use them as far as practicable, meaning as far as an acceptable balance between usability and security is found.

Standard No. 3 "Unless channels of remote e-voting are universally accessible..."

35. Adding additional channels, namely e-voting, to traditional forms of voting may render elections and referendums more accessible and thus strengthen the principle of universality. However, offering the remote e-voting channel exclusively restricts accessibility, given the fact that the channel, namely internet, is not universally accessible for the time being. This provision aims at protecting the voter so that he or she is offered a means of voting which is effectively available to him or to her.

Standard No. 4 "Before casting a vote using a remote e-voting…"

36. When introducing totally new voting methods, especially remote e-voting, voters' attention shall be specifically drawn to the fact that this is an official channel used in a real election or referendum. The aim is to avoid that voters mistakenly imagine that they are taking part in a fake election or referendum or any other test. The same communication effort should be made when using a demonstration or test version, to avoid that voters get the impression that they have already voted. Furthermore, an election or referendum should be clearly distinguished from opinion polls and vice-versa.

EQUAL SUFFRAGE

Standard No. 5 "All official voting information shall be presented..."

37. All official voting information, in particular voting options, shall be presented in an equal way on the different channels. This implies equality of content. Measures should be introduced that prevent both the omission of information that should appear on the electronic ballot and the introduction of any additional information which does not appear on the official ballot, as foreseen by the law.

38. This also implies that there shall be equality with respect to the way information is displayed. However complete equality of display may be difficult or impossible to achieve as different supports (for instance mobile phone, digital TV, e-voting machines or PC) display the information in different ways on their screens. In such a case, it should be recognized that this is not a purely technical matter and should not be left to technical personnel alone to decide. The electoral management body should provide guidance on this matter.

Standard No. 6 "Where electronic and non-electronic voting channels are used..."

39. E-votes are first decrypted and counted. Then the results are aggregated with those obtained from paper votes and the final result is calculated. To do so an aggregation method, probably software, is needed. It must fulfil the same security and reliability objectives as the e-voting software.

40. When the number of e-votes or of paper votes is particularly small there is the risk that vote secrecy may be violated if the results of those few votes are disclosed. The aggregation method should contain the necessary technical and procedural safeguards to ensure consolidation of results of the different

voting channels before results are disclosed, thus ensuring secrecy. In addition, procedural rules, related namely to personnel intervening in the counting process, should take into account such cases.

Standard No. 7 "Unique identification of voters..."

41. Unique identification refers to validating the identity of a specific person by means of one or more features so that the person can unmistakably be distinguished from all other persons. The voters' registers therefore need to provide means to avoid digital twins – i.e. persons holding the same identification data. In cases where central voters' registers are used, unique identification may implicitly be given by the entry of the person in the database. With interconnected voters' registers additional means may be necessary.

42. As someone may be both a voter and a candidate, it is important to prevent the same person having the same identification in the system for all his or her roles. The same applies to people who may be both an administrator of the e-voting system and a voter. Authentication can be identity-based and role-based. While identity-based authentication is advisable for voters registering or casting a vote, or candidate nomination, it might be sufficient to have role-based authentication for administrators, auditors, etc.

Standard No. 8 "The e-voting system shall only grant a user access..."

43. In cases where anonymous voting tokens prove that a voter is eligible to vote, identification of the voter may not be required at this point as it has already taken place at an earlier stage, namely when the specific token is assigned to a specific voter.

Standard No. 9 "The e-voting system shall ensure that only the appropriate number of votes..."

44. All votes cast by either electronic or non-electronic voting channels are counted. It should be ensured that only eligible voters' votes are included in the election result. The principle "one person one vote" shall be respected and only the appropriate number of votes, as foreseen in legislation, is included per voter.

FREE SUFFRAGE

Standard No. 10 "The voter's intention shall not be affected..."

45. The voting system must not influence the eligible voter's intention. The personal exercise of the right to vote is a fundamental principle. As it is vulnerable particularly in the context of remote e-voting, special attention is drawn to this fact. This standard does not prohibit remote e-voting, however adequate provisions should be introduced at the regulatory and implementation levels to ensure that personal and free suffrage is respected. The same is true for non-remote e-voting.

46. In a remote e-voting context, aspects to be considered are the possible faking of an official server by tampering with the domain name system (DNS), the use

of a similar domain name to that of the official e-voting server, man-in-the-middle attacks, or malware in the voter's system that replaces the original ballot or submits counterfeit ballots.

47. Depending on national legislation and policies and in order to ensure accessibility, the principle of universality may be given priority over the principle of personal suffrage and therefore, for example, proxy voting may be allowed. The same conditions apply also to the e-voting channel. However, here again, the rules and conditions for allowing proxy voting shall be respected.

48. Electronic signatures, verifiability codes or other techniques applied to the ballot may allow verifying that the vote has not been tempered with. The use of such techniques shall, however, respect the confidentiality of the vote. At the same time, it should be clearly regulated how to proceed in case the verification shows that the vote has been tampered with.

Standard No. 11 "It shall be ensured that the e-voting system presents an authentic ballot..."

49. In addition to the techniques foreseen under standards 5 and 10, standard 11 requires procedural steps to be introduced to make sure that all information entered in the e-voting and presented to the voter through the e-voting interface is authentic, namely identical to the one provided by the competent authority.

Standard No. 12 "The way in which voters are guided through..."

50. During the voting process, it is important that decisions cannot be taken by inadvertently pressing a button or a link but truly reflect the will of the voter. In particular where e-voting takes place from an uncontrolled environment, the voter should be reminded at the beginning of the process that he or she is participating in a real vote. Throughout the process, both in controlled and uncontrolled forms of e-voting, the voter should be left with enough time to think and react so that he or she is not obliged to vote without reflecting on the choices he or she enters. The design of the interface, messages to the voter and any other relevant aspect should be programmed so as to allow the voter to express his or her true will. At the end of the voting process the voter's choices are summarized and the voter is asked to confirm that the summary reflects his or her true will. Only after this, the vote is sent to the voting server or entered in the electronic ballot box. The detailed implementation of this provision may however vary depending on the specificities of the e-voting system used.

Standard No. 13 "The e-voting system shall provide the voter with..."

51. With paper-based voting systems voters are enabled to participate in the election and yet not to express a preference for the proposed choices. The standard provides that this possibility has to be maintained with e-voting.

52. This standard does not influence the legal validity and effects of a blank vote or of an intentional invalid vote. These issues are regulated at the national level. Countries decide for instance if such votes are accepted, how (if) they are

counted or what is their legal effect on the result. It is a matter for each member State to decide whether such options must be allowed with e-voting as well. Where the "blank vote" option is already foreseen on the paper ballot, it is sufficient if this option is also present on the e-vote ballot. This standard simply forbids a system where a voter is obliged to select one choice (other than blank) in order to complete the voting process. As such, it intends to provide the same guarantees than paper-based systems, where a voter does have the choice not to choose any proposed candidate for instance.

Standard No. 14 "The e-voting system shall advise the voter..."

53. As explained in the previous paragraphs, this Recommendation does not prevent member States from introducing other voting options such as the possibility intentionally to cast an invalid vote. Furthermore, intentionally valid votes may, under specific circumstances, be invalidated namely due to technical complications without the voter necessarily being aware of this fact. The present standard does not require that the invalid voting possibility is introduced as a voting option. It only requires that, whenever an invalid vote is received by the e-voting system, for whatever reason, the voter that issued that vote shall be informed accordingly. The aim is to avoid unintentional invalid e-votes. It applies in all cases, whether the e-voting system allows or disallows invalid votes. Of course, it only applies to votes cast electronically.

54. When advising the voter that his or her vote is invalid, the system should also inform him or her on the consequences of such invalidity (is it considered or not, etc.) as well as the possibility to cast a new vote if the invalidity is unintentional. If a system does not accept invalid votes, the ballot may be refused, or taken and discarded. If the system accepts invalid votes, it will be accepted pending reaction of the voter: if the invalidity is unintentional, the voter may want to cast a new vote; otherwise he or she has issued an intentionally invalid vote and maintains that choice. A lot depends in this case on the national regulation of invalid votes. The advantage of an e-voting system is that it is possible to inform and for the voter to react to such invalidity when it does not reflect his or her true will.

Standard No. 15 "The voter shall be able to verify that..."

55. Standards 15 to 18 introduce verifiability mechanisms which develop the concept of chain of trust in e-enabled elections. Standard 15 refers to verifiability tools which enable the voter to verify that his or her e-vote was cast as intended and recorded as cast, also known as individual verifiability. Individual verifiability tools vary depending on the specific e-voting solution. The voter verifiable paper audit trail produced by an e-voting machine used in a polling station or the return codes used in internet voting are examples of such tools.

56. Standard 16 is about confirmation by the system that the voting procedure was completed successfully. Standard 17 refers to verifiability tools which allow any interested person to verify that votes are counted as recorded (universal verifiability) and standard 18 provides that it is possible to verify that only eligible voters' votes were included in the final result, thus completing the chain of trust.

Standard No. 16 "The voter shall receive confirmation..."

57. The voting procedure is completed successfully when the electronic vote is deposited in the electronic ballot box. In the context of remote e-voting this means that the voting procedure is completed successfully only when the vote has been sent from the voter's voting device (PC, telephone, etc.), over the internet or another network and has reached its destination, i.e. the ballot box server.

58. The system confirms to the voter that his or her vote is deposited in the ballot box and will be counted and that the voting process is completed successfully. From the moment the voter learns this, he or she can safely log out or break the connection. Both messages on the successful casting of the ballot and on the completion of the procedure can be combined into one message, if the two events coincide. It is good practice to accompany these messages with a reminder and instructions to the voter on how to delete traces of the vote if voting was done from an uncontrolled device.

Standard No. 17 " The e-voting system shall provide sound evidence that each authentic vote..."

59. The voting system ensures that each vote is correctly included in the election result. This requires the ability to provide sound evidence to voters and third parties that the results are a true and accurate representation of the authentic votes cast and meet the legal requirements of democratic elections and referendums. "Sound evidence" refers to criteria for such evidence to be broadly accepted. "Authentic votes" refers to previously mentioned standards which make sure that the vote reflects the free will of the voter.

60. Furthermore, it should be possible to audit the evidence to verify its correctness with tools which are external to and independent from the e-voting system. To do so, the e-voting system should provide interfaces with comprehensive observation and auditing possibilities, subject to the needs of secrecy and anonymity of the vote.

61. The percentage of votes cast by e-voting and the comparison of the results of e-voting versus the results of voting by other channels can be considered to establish the plausibility of the correctness of the e-voting results.

Standard No. 18 "The system shall provide sound evidence that only eligible voters'..."

62. Voters and third parties should be able to check that only eligible voters' votes are included in the election result. At the same time counted votes should be anonymous. In the case of internet voting, there exist encryption methods that do not require decoding before votes are counted (homomorphic encryption). Counting can be performed without disclosing the content of encrypted votes.

SECRET SUFFRAGE

Standard No. 19 "E-voting shall be organised in such a way..."

63. This standard sets the general requirement of secrecy of the vote which applies throughout the entire procedure: in the pre-voting stage (e.g. transmitting of PINs, or electronic tokens to voters), during the completion of the ballot paper, the casting and transmission of the ballot and during counting and any recounting of the votes.

64. The necessary measures include of course encryption, but also, for example, that the votes cast are mixed in the electronic ballot box so that the order in which they appear at the counting phase does not allow reconstruction of the order in which they arrived.

Standard No. 20 "The e-voting system shall process and store..."

65. The voting system shall only process and store the personal data without which the system does not operate correctly. This requirement, also called "data minimisation", refers to data necessary for fulfilling legal requirements of the voting process. The electoral management body in charge of organising e-voting identifies such data and should be able to explain what are the underlying legal provisions and considerations that render them necessary. The duration of processing, storing etc. also depends on legal requirements, namely those related to appeals. Data minimisation aims at ensuring data protection and is part of vote secrecy.

Standard No. 21 "The e-voting system and any authorised party..."

66. Domestic legislation may foresee different ways of identification and authentication for different voting channels (indication of the voter's name, showing of an ID-Card, use of codes which are specific to each voter, etc.). The overall aim is to ensure that only people with the right to vote can effectively vote and to prevent multiple votes or other misuse.

67. The standard implies that the system itself and any authorised party do at some point handle authentication information. An example of authorised party is the entity that prints the voting material which contains authentication information. The system and any authorised party should protect this information through technical and organisational means. Anyone else, by definition unauthorised party, should not access or otherwise use this data.

68. Other services, such as information services for the voter prior to entering the voting process, which clearly do not need authentication, are outside the scope of this standard.

Standard No. 22 "Voters' registers stored in or communicated by the e-voting system..."

69. This standard provides that only authorised parties have access specifically to voters' registers.

Standard No. 23 "An e-voting system shall not provide the voter..."

70. The aim of this standard is to prevent the breach of vote secrecy as well as vote selling. However, individual verifiability can be implemented provided adequate safeguards exist to prevent coercion or vote-buying.

71. Provisions that handle cases of breach of vote secrecy or vote selling should be in place. In many countries criminal law provisions deal with such violations. They cover all voting channels used and should apply also when e-voting is used. If necessary they should be updated to take into account e-voting specificities.

72. Where paper proof of the content of the vote is produced, as this happens in controlled environments where electronic voting machines are used, technical and organisational measures should be in place that prevent the voter from making any use of that proof other than the normal use foreseen during the voting process. The voter cannot for instance use the proof to breach vote secrecy or take it with him or her outside the supervised place.

73. In a remote e-voting system using the internet, the voter should be informed on the necessity to delete traces of the voting transaction from the device used to cast the vote and on how to do so. Such traces could be kept for instance in the personal computer's memory, the browser cache, the video memory, swap files, temporary files, etc.

74. Specific attention should be paid to the way in which the anonymity and secrecy of the vote are implemented when designing an e-voting system. With respect to remote e-voting, there are at least three layers to be considered: the web application, the browser and the utility software on the computer of the voter.

- a. The web application should not allow the user to retain a copy of his or her vote. It should not offer the functionality of printing, saving or storing the vote or (part of) the screen on which the vote is visible.
- b. The browser should not offer the option of printing the screen on which the vote is visible. It should be noted that browsers can and do retain information in several ways. For example, by using the "back" button on a browser, one or more previous screens can be displayed. As far as possible, this generic functionality of browsers should be disabled by the web application. At the very least, there should be no storing of information after the voter has finished casting the vote.
- c. Pieces of software that can record in some way what actions a specific user of a computer has performed have to be accounted for. Three common examples are screen shot utilities, utilities that make films of the sequence of screens and utilities that record the key strokes a user makes. Such software can be present as malware in the user's computer, without the user's knowledge. The e-voting system may not be able to prevent the presence of such malware. The voter should be informed about the possibility of such malware, the potential risks they present, the good practice to be adopted by him or her to minimize the risks and, more generally, about alternative and more secure voting channels that are open to him or her.

Standard No. 24 "The e-voting system shall not allow the disclosure..."

75. This standard aims at preventing the establishing and publication of intermediary results of the e-voting channel. Information about participation levels falls outside the scope of this standard and can be collected and released as foreseen by national regulations.

Standard No. 25 "E-voting shall ensure that the secrecy of previous choices..."

76. This standard requires that the secrecy of previous choices which were entered and then deleted by the voter during the voting process shall receive the same protection as the secrecy of the final vote.

Standard No. 26 "The e-voting process, in particular the counting stage..."

77. This standard provides that it must not be possible to link the vote to the voter who cast it and thus prevents vote secrecy breaching.

78. In non-remote e-voting processes the voter authentication and the vote can be separated physically also when e-voting systems are used. This physical separation can, in principle be controlled by election officials and election observers, assuming that there is deliberate or inadvertent error in the e-voting system (and no malware).

79. In the remote voting process, information linked to the voter (usually a code) and the votes are connected up to a certain stage. In countries that allow multiple voting, this link is necessary to handle multiple votes and their effect (a vote erases another). The separation has to be made electronically at a predefined stage before counting takes place. This requires specific technical solutions.

80. In cases where domestic law requires a permanent link between the voter and the vote to exist and to be maintained during the election or referendum and for a specific period thereafter, it has to be assured that the link between a voter and his or her ballot is sufficiently protected throughout the period in order to ensure the secrecy of the vote. This is only revealed pursuant to an order of a competent judicial authority and it must be ensured, that even where the link is so revealed, no voter is compelled to reveal how he or she has voted.

81. An audit system should maintain voter anonymity at all times, except when specifically required otherwise under domestic legal provisions. In all cases the information gathered by the audit system has to be protected against unauthorised access.

REGULATORY AND ORGANISATIONAL REQUIREMENTS

Standard No. 27 "Member States that introduce e-voting..."

82. Electronic voting technologies should be introduced in a gradual, step-by-step manner and tested under realistic conditions prior to Election Day. According to member States' experience, the gradual introduction is necessary given the legal and technical challenges and opportunities that e-voting presents. Some of the main steps are described in the guidelines related to this standard.

83. In particular, other forms of remote voting such as postal (correspondence) voting, should be well established and trusted before introducing remote e-voting. Many operational and user-confidence issues related to remote e-voting are similar to those related to postal voting and can be more easily addressed in the context of postal voting.

Standard No. 28 "Before introducing e-voting, member States..."

84. While this standard may look obvious at first sight, the aim is to call member States' attention to the fact that in addition to regulating the details of e-voting, they may need to change the law or even the constitution to allow for e-voting. Existing legislation is not written with automation in mind and may be ambiguous when applied to e-voting.

85. Another lesson learned from experiences in the region is that e-voting specific regulations need to be detailed to allow any stakeholder concerned to understand e-voting and to conduct his or her own functions in relation to it. Detailed regulations are furthermore important to guarantee that the implementation of technology complies with the principles for democratic elections and referendums.

86. The legal framework should provide for judicial review of e-voting which allows citizens to challenge the actual method used for e-voting, as well as the implementation of the method, thus increasing public confidence and trust in e-voting.

Standard No. 29 "The relevant legislation shall regulate the responsibilities..."

87. There are numerous stakeholders that play a role and bear some degree of responsibility in developing, testing, certifying, deploying, applying, maintaining, observing and auditing e-voting systems. Ultimately, however, it is the government that bears the overall responsibility for the voting and thus for the e-voting system. It is recommended that the relevant legislation provides for the supervisory role of the electoral management body over e-voting. The role and the responsibilities of the other parties involved should be clarified at the appropriate regulatory or contractual level.

88. One aspect which will help make sure that the electoral management body has effective control over e-voting is for member States not to be over dependent on just a few vendors since this could result in a vendor-lock-in. Indeed, software and hardware of an e-voting system require ongoing maintenance. This is in addition to the procedures required for a specific event, for example the creation of ballot papers. When considering outsourcing, it is essential that those who are responsible for the elections understand what is being outsourced, why it is being outsourced and what methods and processes the vendor intends to undertake. Statutory duties of the body responsible for the conduct of elections must never be outsourced, since this body is in charge of the election.

Standard No. 30 "Any observer shall be able to observe the count of the votes. The electoral management body shall be responsible for the counting process."

89. The aim of this standard is to underline the role of the electoral management body in the counting process, not only as one of the participants but as the organiser and supervisor of the counting. The presence of observers should be provided for. Such observers should include representatives of political parties as well as the general public.

TRANSPARENCY AND OBSERVATION

Standard No. 31 "Member States shall be transparent in all..."

90. An e-voting system can only be introduced if voters have trust and confidence in their electoral system and in election administration. However, trust should not be taken for granted and states need to do their utmost in order to ensure that it is preserved. Fostering transparent practices in member States is a key element for building public trust and confidence. Being transparent about the e-voting system, the processes surrounding it and the reasons for introducing e-voting will contribute to voters' knowledge and understanding, thereby generating trust and public confidence.

91. This standard provides for broad transparency on all aspects of all forms of e-voting. In particular system's transparency, or the possibility to check that it is functioning properly, must be guaranteed. Member States regulate who has access to what and when and under what circumstances.

92. Transparency can furthermore be achieved by being open about the e-voting procedure. In addition to the electronic voting system, member States should also ensure transparency regarding all procedures (before, during and after Election Day/period) related to e-voting. This can be done by publishing illustrations (e.g. photos, videos, etc.) on the official website that explain e-voting to all interested parties. The use of sign language and subtitles should also be included to further reduce barriers when communicating on e-voting.

93. Representatives of people with disabilities should be involved in the process of introducing e-enabled elections so as to see how this could affect the people they represent.

Standard No. 32 "The public, in particular voters, shall be informed..."

94. An e-election can differ from an election or referendum without e-voting, namely with regard to the procedures that have to be followed by voters. Examples of potential differences are the period of time during which votes can be cast, the steps a voter has to take in order to participate in the e-election and the way the e-voting actually takes place. These differences should be communicated to the voter in order to avoid any misunderstanding of the procedures and in order to give the voter all the information necessary on the use of the e-voting channel. Careful consideration should be given to deciding how much time the voter needs for this decision. Consideration should also be given to offering the voter the opportunity to try the suitability of his or her equipment before he or she decides to use a specific electronic voting channel.

Standard No. 33 "The components of the e-voting system shall be disclosed..."

95. Assessment that e-voting systems function correctly and that security is maintained is essential. The means to achieve this is the independent evaluation or certification of the system as a whole or of its components, which requires disclosure of the critical system elements. The assessment can be accomplished for instance by disclosing the system design, by allowing inspection of the detailed documentation, by disclosing the source code, by allowing inspection of component evaluation and certification reports, in-depth penetration testing, etc. The actual level of disclosure of the elements of the system, necessary for achieving appropriate assurance, depends on the peculiarities of the system, its components and the services provided.

Standard No. 34 "Any observer, to the extent permitted by law, shall be enabled..."

96. Although the availability of documents to the public is important, it will not be possible for everybody to understand an e-voting system. In order to have confidence, voters rely on others who are in a position to understand the materials and the processes. It is therefore essential that observers have as much access as possible to relevant documents, meetings, activities etc.

97. There are various international and domestic election observations. Observers should include representatives of candidates and political parties as well as the general public, both domestic and international independent observers. All member States are bound to the commitments of the Document of the Copenhagen Meeting of the Conference on the Human Dimension of the OSCE of 29 June 1990 to "invite observers from any other OSCE participating state and any appropriate private institution and organisation who may wish to do so to observe the course of their national election proceedings [… and …] facilitate similar access for election proceedings held below the national level." Procedures for accepting observers, as well as rights and obligations of observers are defined by the respective country's legislation and should respect the international commitments of the country.

98. Observers, to the extent permitted by law, should be able to verify that the e-voting system itself is designed and operated in a way which respects the fundamental principles of democratic elections and referendums. Therefore, member States should have clear legal provisions on observers' access to the e-voting system documentation and audit data.

99. E-voting poses special challenges to observers, inherent to the electronic conduct of the election or referendum. Observers will thus have to be provided with an opportunity, in particular, to have access to relevant software information, to see physical and electronic safety measures for servers, to inspect and test certified devices, to have access to and test, sites and information provided for remote e-voting, and to observe electronic votes cast and those that are being counted. Security measures may, however, make it necessary not to allow the presence of observers in the computer room itself. In that case measures should be taken in order to give the observers the opportunity to monitor the activities.

Standard No. 35 "Open standards shall be used to enable various technical..."

100. In order to be able to use e-voting systems or services from different suppliers, these must be interoperable. Interoperability means that the input and output conform to open standards and especially open standards for e-voting. Such standards need to be updated on a regular basis to take account of legal and technical developments.

101. The main benefits of using open standards are:

- Greater choice of products and suppliers
- Less dependency on a single supplier
- Avoidance of proprietary lock-in
- Stability or reduction in costs
- Easier accommodation of future changes

102. Countries, in particular decentralised ones with a variety of states/members and thus a variety of electoral practices, may decide to adopt such standards at the country level.[5] At the regional level, countries may decide to adopt regional standards.

103. At the international level, OASIS, the International e-Business interoperability consortium, developed standards for election and voter services information using XML. OASIS elaborated the Election Markup Language (EML). EML is a set of data and message definitions described as XML schemas. It was the first international standard for the structured interchange of data among hardware, software, and service providers who engage in any aspect of providing election or voter services. Its function is to ensure open, secure, standardised and interoperable interfaces between the components of election systems. Further information on OASIS work on elections (which ended mid 2015) is available at www.oasis-open.org/committees/election.

ACCOUNTABILITY

Standard No. 36 "Member States shall develop technical, evaluation..."

104. Election management bodies or the entity designated by them should develop technical requirements for e-voting systems. They should furthermore develop requirements for evaluation techniques ranging from testing to formal certification of e-voting systems. Common Criteria Protection Profiles and Common Criteria CC/ISO 15408 contain such kind of requirements.

105. Both types of requirement aim at ensuring, already before the effective use of the e-voting system in an election or referendum, that the system is designed in conformity with requirements for democratic elections and that it operates correctly, namely does exactly what it is supposed to do.

106. It's up to the election management body or the designated entity to make sure that all mentioned requirements fully reflect the relevant legal principles for democratic elections. This implies that requirements are updated as often as

5. This is the case for instance in Switzerland, where standards have been introduced by eCH, the e-Government standards setting association. Further information on e-voting related standards is available www.ech.ch under eCH Documents > nach Themenbereich > Politische Aktivitäten.

necessary to integrate possible legal developments. For example, the organisational rules of a type of election may change over time: so should also the respective requirements that translate such rules into technical instructions for the system or for its certification.

Standard No. 37 "Before an e-voting system is introduced and at appropriate..."

107. An appropriate control of an e-voting system provides evidence as to the compatibility of the system with technical requirements which, as mentioned in the previous provision, are derived from, and aim at implementing principles for democratic elections. The added value of such a control is not only to establish if an e-voting system is in compliance with the prescribed requirements and standards; it is also an important tool in the establishment of trust on the e-voting system.

108. The election management body must ensure that the e-voting system complies with technical requirements. To do so, it should charge an independent and competent body to evaluate the system. The notion of an independent body covers both independence from the system manufacturer or service provider and independence from political interference.

109. The independent body may be a governmental one, such as an agency in charge of national IT security certification. It may be a private (national or international) organisation such as evaluation laboratories or certification bodies (for instance those that are accredited for the national or international evaluation schemes such as BS7799/ISO17799, Common Criteria, or ITSEC). Whichever the case, such a body should be competent to conduct the certification work, in addition to being independent from the manufacturer/ service provider and from political interference. Furthermore, its designation (as a certification body) should be transparent.

110. Certification or any other appropriate control is done before the e-voting system is introduced and at appropriate intervals whenever necessary, namely after important changes in the system. Certification can be applied in different ways. Member States may choose for instance to certify the whole system or only components of it, bearing in mind the need to ensure that the voting system and procedures should be able to respond to possible threats and risks and respect standards for democratic elections and referendums.

Standard No. 38 "The certificate, or any other appropriate document..."

111. Any appropriate document issued should make the evaluation process and the outcome transparent and reproducible for third parties especially those that have access to the system. Based on the certificate it should be possible to verify that the system used for the election is the one that was certified. Therefore the certificate should at least include (or refer to) the following information:

- Issuer;
- Validation period/ date/ conditions (e.g. non-disclosure agreement);

- Description of the purpose of the certificate. Does the certificate declare if the system is accessible, secure, usable, functionally correct, and to what extent;
- Description of the method of the certification process. What standards are used? What methods are used for testing and evaluating a system? How is source code reviewed? How are hardware components checked?;
- Description of the certified system. To ensure reproducibility for third parties this has to include digital fingerprints of software components, detailed specifications of firmware versions, hardware components, etc.;
- Outcome of the certification process;
- Comments about operational requirements or other preconditions;
- A digital fingerprint of the certificate or a similar system.

Standard No. 39 "The e-voting system shall be auditable..."

112. Auditing of the e-voting process, resources or infrastructure is a means to establish trust and confidence in the operation of the ICT system(s) used for e-voting. It requires integrity and authenticity of the audit information and of the deployed auditing systems.

113. Audits aim at detecting possible attacks on systems. Independent and extensive security monitoring, auditing, cross checking and reporting are a critical part of e-voting systems. E-voting systems should therefore have audit facilities for each of the main components (vote, count, etc.) and on different levels of the system: logical, application, technical.

114. Audit facilities on the logical level should report upon the use that is being made of the system. Audit facilities on the application level should give information on the activities that the system supports in order to enable reconstruction of the system's operation. Audit facilities on the technical level should provide information on the activities that the infrastructure that is being used supports. This varies from routine information on, for example, specific load information and system malfunction, to specific information on the signals an intrusion detection system (IDS) gives with regard to possible attacks.

115. Audit trails are critical for e-voting systems, so they must be as comprehensive as possible and open to scrutiny by authorised third parties. Audited data should be provided at various points and levels within an electronic voting system, for example data can be audited at the EML, IT system or communications infrastructure levels.

116. At the EML level for instance there are many standardised open interface points. Data flows at these interface points can be easily observed and monitored. Audit systems should also cover non EML interfaces, for example

interfaces within the communications infrastructure, databases and system management functions.

117. There should be procedural requirements specified for the use of audit systems while election or referendums are running and predetermined procedures for rapid response scenarios.

118. The audit system should provide the ability for any observer to monitor the real time progress of the election or referendum without revealing the potential end count/result. For example, observers should be able to see the total number of ballots being cast in real time, so that independent cross checks can be performed.

119. The audit system should be able to detect voter fraud and provide proof that all counted votes are authentic. All occurrences of attempted voter fraud should be logged; the audit system logs should contain data that provides the ability to cross check credentials giving the right to vote and shall ensure that all counted votes were cast by a voter with a right to do so and that all authentic votes have been counted as such.

120. The audit system should include all election or referendum data required by electoral officials to cross reference and account for all cast ballots, thereby verifying the correct operations of the voting system and the legitimacy of the result. A count of ballots is required to match the total votes cast, including valid and invalid votes. The audit system should give information to facilitate an independent cross check and verify the correct operation of the e-election or e-referendum system and the accuracy of the result. The audit system should be able to ensure that no authentic votes are lost and that there are no votes that are unaccounted for.

121. Cross checking of independent audit information increases the likelihood of detection of hidden attacks on e-voting systems, as the attack has to be hidden in a consistent way on both the e-voting system and the independent audit information.

122. The audit system should meet the same security requirements specified for the implementation of the e-voting system itself.

123. The audit system shall itself be protected against attacks intended or likely to corrupt, alter or lose records. Detection of any insider or outsider attacks on the audit system shall be reported and acted on immediately.

RELIABILITY AND SECURITY OF THE SYSTEM

Standard No. 40 "The electoral management body shall be responsible..."

124. In addition to being available and usable, the e-voting channel needs to be reliable and secure to comply with the principles for democratic elections. It is the member State who has to guarantee that this is the case. The overall responsibility falls on the electoral management body that supervises e-voting and cannot be delegated for instance to a voting system supplier.

125. Respect for the principles shall be ensured also in the presence of failures or attacks. This implies that the e-voting system shall be secure, i.e. robust as to withstand deliberate attack, and reliable, i.e. able to function on its own, irrespective of shortcomings in the hardware or software.

126. Technical solutions that reflect state of the art, are peer-reviewed and broadly endorsed by the respective scientific community help ensure availability, reliability, usability and security of the e-voting system even in the presence of failure and attacks.

Standard No. 41 "Only persons authorised by the electoral management body..."

127. Any intervention on hardware or software carries intrinsic technical and human risks, which should be kept to a minimum while an operation is in progress. That is why automatic controls are to be preferred and limitations placed on remote manipulations without official supervision. If there is a necessity to intervene, the risks of intrusion, human error, sabotage, etc. are to be reduced as far as possible. This should be done by establishing a working procedure to be followed and validated, which restricts the number of persons authorised to do the work to a small supervised group and requires the verification of each act through the physical presence of two or more qualified persons. Those persons should comply with the security rules laid down by the competent authority.

Standard No. 42 "Before any e-election takes place, the electoral management body..."

128. Before any e-election takes place, the electoral management body shall satisfy itself that the e-voting system used is actually the system that is supposed to be used, that is, that the software is genuine (the same as the one previously checked and authorised for use) and operates correctly.

129. Verification should prevent any e-voting system being installed if the system or any of its components have been tampered with or have been replaced. The electoral management body needs to ensure that the correct system is put into service. Furthermore, the standard requires that the system operates correctly.

Standard No. 43 "A procedure shall be established for regularly..."

130. Constant development in information and communication technologies renders regular updates (particularly) of software necessary. This calls for updates to central systems and voting facilities used in a controlled environment (for example, voting machines). Any important update needs to be certified similar to the initial certification before being brought into operation.

131. It is essential that electronic voting systems remain as transparent as possible for authorities and citizens alike. Exact, full, up-to-date descriptions of the hardware and software components should be published, thus enabling interested groups to verify for themselves that the systems in use correspond to the ones certified by the competent authorities. The results of certification should be made available to the authorities, political parties and, depending on legal provisions, citizens.

Standard No. 44 "If stored or communicated outside controlled environments..."

132. From the moment the vote is cast, no one should be able to change it or relate the vote to the voter who cast it. This is achieved, among other measures, by the process of sealing the ballot box, and where the ballot box is remote from the voter by sealing the vote throughout its transmission from voter to ballot box by using encryption. A vote is sealed when its content has been subject to the measures that ensure that it cannot be read, changed, or related to the voter who cast it.

133. To seal and protect an electronic ballot box, physical and technical measures may be necessary, such as control of access, authorisation structures and firewalls.

Standard No. 45 "Votes and voter information shall be kept sealed..."

134. This clarifies the moment where sealing ends: just before the counting. As mentioned elsewhere (and by analogy with the physical ballot box), before unsealing, votes are mixed.

Standard No. 46 "The electoral management body shall handle..."

135. This standard reminds that adequate, state of the art procedures must be foreseen for the handling of cryptographic material.

Standard No. 47 " Where incidents that could threaten the integrity of the system..."

136. It is important that incidents that threaten the integrity of the system are reported immediately to the competent entity in charge of communication which makes sure that the necessary measures are taken and all interested stakeholders, namely political parties and voters are properly informed.

Standard No. 48 "The authenticity, availability and integrity of the voters' registers..."

137. Data-origin authentication can for example be provided by electronic signatures in fully electronic processes. In semi-electronic processes, data-origin authentication may employ also conventional security measures, such as manual signatures, seals, couriers, etc.

138. The voters register may not be required in the e-voting system if, in a two-phase model, an anonymous voting token is used to establish the right to vote. It is to be noted that voters' registers in the polling station might be needed to prevent multiple votes (electronically and on paper-ballot) or where voting is compulsory and thus a list of those who have voted is essential.

Standard No. 49 "The e-voting system shall identify votes..."

139. Irregularities shall be identified so that the necessary measures are taken and stakeholders (voter, electoral management body, etc.) can be informed and are able to react accordingly.

Guidelines[1]

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

(Adopted by the Committee of Ministers of the Council of Europe on 14 June 2017 at the 1289th meeting of the Ministers' Deputies)

Ad hoc Committee of Experts on Legal, Operational and Technical Standards for e-voting (CAHVE)

(Item considered by the GR-DEM at its meetings on 20 April and 1 June 2017)

PREAMBLE

The Committee of Ministers, under the terms of Article 15.b of the Statute of the Council of Europe,

Considering that the aim of the Council of Europe is to achieve a greater unity between its members for the purpose of safeguarding and promoting the ideals and principles which are their common heritage;

Reaffirming its belief that representative and direct democracy is part of that common heritage and is the basis of the participation of citizens in political life at the level of the European Union and at national, regional and local levels;

Having regard to the obligations and commitments as undertaken within existing international instruments and documents, such as:

- the Universal Declaration on Human Rights;
- the International Covenant on Civil and Political Rights;
- the United Nations Convention on the Elimination of All Forms of Racial Discrimination;
- the United Nations Convention on the Elimination of All Forms of Discrimination against Women;
- the United Nations Convention on the Rights of Persons with Disabilities;

1. Source: www.coe.int/cm

- the United Nations Convention against Corruption;
- the Convention for the Protection of Human Rights and Fundamental Freedoms (ETS No. 5), in particular the Protocol thereto (ETS No. 9);
- the European Charter of Local Self-Government (ETS No. 122);
- the Convention on Cybercrime (ETS No. 185);
- the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (ETS No. 108);
- the Additional Protocol to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows (ETS No. 181);
- the Convention on the Standards of Democratic Elections, Electoral Rights and Freedoms in the Member States of the Commonwealth of Independent States (CDL-EL(2006)031rev);
- Recommendation No. R (99) 5 of the Committee of Ministers to member States on the protection of privacy on the Internet;
- Recommendation Rec(2004)15 of the Committee of Ministers to member States on electronic governance (e-governance);
- Recommendation CM/Rec(2009)1 of the Committee of Ministers to member States on electronic democracy (e-democracy);
- the document of the Copenhagen Meeting of the Conference on the Human Dimension of the OSCE;
- the Charter of Fundamental Rights of the European Union;
- the Code of Good Practice in Electoral Matters, adopted by the Council for Democratic Elections of the Council of Europe and the European Commission for Democracy through Law (Venice Commission) and supported by the Committee of Ministers, the Parliamentary Assembly, and the Congress of Local and Regional Authorities of the Council of Europe;

Bearing in mind that the right to vote lies at the foundations of democracy, and that, consequently, all voting channels, including e-voting, shall comply with the principles of democratic elections and referendums;

Recognising that the use of information and communication technologies by member States in elections has increased considerably in recent years;

Noting that some member States already use, or are considering using e-voting for a number of purposes, including:

- enabling voters to cast their votes from a place other than the polling station in their voting district;
- facilitating the casting of the vote by the voter;

- facilitating the participation in elections and referendums of citizens entitled to vote and residing or staying abroad;

- widening access to the voting process for voters with disabilities or those having other difficulties in being physically present at a polling station and using the devices available there;

- increasing voter turnout by providing additional voting channels;

- bringing voting in line with new developments in society and the increasing use of new technologies as a medium for communication and civic engagement in pursuit of democracy;

- reducing, over time, the overall cost to the electoral authorities of conducting an election or referendum;

- delivering voting results reliably and more quickly;

- providing the electorate with a better service, by offering a variety of voting channels;

Valuing the experience gathered by the member States that have used e-voting in recent years and of the lessons learned through such experience;

Aware also of the experience resulting from the application of Recommendation Rec(2004)11 of the Committee of Ministers to member States on legal, operational and technical standards for e-voting, the Guidelines for developing processes that confirm compliance with prescribed requirements and standards (Certification of e-voting systems) and the Guidelines on transparency of e-enabled elections;

Reaffirming its belief that public trust in the authorities in charge of managing elections is a precondition to the introduction of e-voting;

Aware of concerns about potential security, reliability or transparency problems of e-voting systems;

Conscious, therefore, that only those e-voting systems which are secure, reliable, efficient, technically robust, open to independent verification and easily accessible to voters will build public confidence, which is a pre-requisite for holding e-elections;

Aware of the need for the member States to take into account the environment in which e-voting is implemented;

Aware that, in the light of recent technical and legal developments on e-enabled elections in Council of Europe member States, the provisions of Recommendation Rec(2004)11 need to be thoroughly revised and brought up to date;

Having regard to the work of the Ad hoc Committee of Experts on Legal, Operational and Technical Standards for e-voting (CAHVE) set up by the Committee of Ministers with the task of updating Recommendation Rec(2004)11;

Adopts the following guidelines on e-voting standards to serve as a practical tool for the governments of the member States in endorsing, adopting, implementing and monitoring the e-voting approach described therein and adapting their e-voting systems;

Invites the governments of the member States to ensure that the guidelines are widely disseminated among electoral management bodies, election officials, citizens, political parties, domestic and international observers, non-governmental organisations (NGOs), media, academics, providers of e-voting solutions and specific e-voting controlling bodies.

INTRODUCTION

1. The present guidelines are the updated version of the Guidelines for developing processes that confirm compliance with prescribed requirements and standards (Certification of e-voting systems) and the Guidelines on transparency of e-enabled elections. The original two guidelines were approved in 2011 with the aim of providing guidance on how to implement the provisions on certification and transparency of Recommendation Rec(2004)11 of the Committee of Ministers to member States on legal, operational and technical standards for e-voting of 30 September 2004.

2. The Recommendation Rec(2004)11 and the original guidelines were reviewed and updated in 2015 and 2016 by the Ad hoc Committee of Experts on Legal, Operational and Technical Standards for e-voting (CAHVE), set up by the Committee of Ministers on 1 April 2015.

3. The present guidelines provide guidance on the implementation of the provisions of the Recommendation CM/Rec(2017)5. Each of the guidelines is identified by a number, which refers to the corresponding provision in the recommendation.

4. The present version of the guidelines is a work in progress that will be further completed to address all forms of e-voting covered by Recommendation CM/Rec(2017)5. Therefore, on-going developments in the legal and technical fields will require that the provisions of the guidelines be updated on a regular basis.

5. The guidelines are designed for use in political elections and referendums at all tiers of governance. They are not intended as a strict set of rules for member States, imposing a particular way of implementing the provisions of the updated recommendation, but are intended to provide guidance and to support member States on the subject.

6. The guidelines, like the updated recommendation, are not an exhaustive regulatory framework for e-voting. Member States need to further develop these provisions to take account of national specificities in the electoral field.

The guidelines also include examples of effective implementation of standards in specific contexts, called "good practice". Examples of good practice are included for information purposes.

I. Guidelines for the implementation of universal suffrage recommendations

1. The voter interface of an e-voting system shall be easy to understand and use by all voters.

- a. The presentation of the voting options on the device used by the voter should be optimised for the average voter who does not have specialised computer knowledge.

  Products and services must be adaptable to the users' functional restrictions and specific circumstances without infringing on principles such as equality. This can be achieved by offering different versions of the same product, changes to key parameters, modular design, ancillaries or other methods.

- b. Voters should be involved in the design of e-voting systems, particularly to identify constraints and test ease of use at each main stage of the development process.

  Accessibility implies that systems are designed in such a way that as many voters as possible can use them. IT- Products and services must be functional and take into account the needs of the public, without being unnecessarily complicated. Such requirements might be achieved with a collaborative approach involving the development team and a representative panel of users.

- c. Consideration should be given, when developing new IT-products, to their compatibility with existing ones.

2. The e-voting system shall be designed, as far as is practicable, to enable persons with disabilities and special needs to vote independently.

- a. Voters should be supplied, whenever required and possible, with additional facilities, such as special interfaces or other equivalent resources, such as personal assistance.

  E-voting can be an alternative way of voting that provides additional possibilities to people with disabilities and special needs to vote independently. An acceptable balance should be found between providing such access possibilities and respecting other requirements, namely those on the security of e-voting.

- b. Internet voting interfaces should comply as much as possible with the guidelines set out in the Web Accessibility Initiative (WAI).

  The World Wide Web Consortium (W3C) was created in 1994 to lead the World Wide Web (WWW) to its full potential by developing common protocols. It initi-

ated the WAI to promote a high degree of accessibility for people with disabilities. The WAI pursues web accessibility through five main areas of work: technology, guidelines, tools, education and outreach, and research and development. WAI has produced a set of standards and guidelines in support of accessibility (for example, web content accessibility guidelines, authoring tools, accessibility guidelines, user agent, accessibility guidelines, XML accessibility guidelines). More information is available from the WAI web site at www.w3.org/WAI.

WAI is commonly used in the context of browser-based solutions for internet voting. Even when internet voting uses alternative solutions (for example, the voting application is a separate unique "browser" in itself), WAI general principles can be followed.

II. Guidelines for the implementation of equal suffrage recommendations

5. All official voting information shall be presented in an equal way, within and across voting channels.

- a. The electronic ballot used for e-voting should be free from any information about voting options, other than that required by law.

  The e-voting interface should not contain more information about the choices than the official (usually paper) ballots. Elements such as pop-up screens that promote a specific candidate or position, or audio elements that are associated with a particular candidate or point of view, and any other information which does not appear on the paper ballot (equality of voting channels) should not appear on the e-voting interface. This does not prevent the display of official information on voting options.

- b. If information about voting options is accessible from the e-voting site, it shall be presented in an equitable manner.

  Information about voting options should be presented in an equitable manner in all voting channels.

9. The e-voting system shall ensure that only the appropriate number of votes per voter is cast, stored in the electronic ballot box and included in the election result.

- a. If a voter is allowed to cast an electronic vote multiple times, appropriate measures should be taken to ensure that only one vote is counted.

- b. If a voter is allowed to cast a vote by more than one voting channel, appropriate measures should be taken to ensure that only one vote is counted.

  Guidelines 9a and 9b: Wherever multiple voting is allowed this should also be reflected in e-voting. For instance, certain voting systems allow voters to submit an advance vote, or several advance votes, and change their minds later. Only the last vote is inserted into the ballot box and thus is the vote cast. This is the case in Andorra, Denmark and Sweden.

The multiple voting option (multiple e-votes or multiple votes via more than one voting channel) may be introduced with e-voting, as a countermeasure to voter coercion, which remains possible when voting takes place outside a controlled environment (remote voting). This is the case in Estonia.

The determination of which vote should be counted is to be made at national level. In an e-voting context, a country may decide that the paper vote has priority. Elsewhere only the last vote cast will be counted. A third country may decide that the first validly issued vote is the one that counts. To be in line with the principles of democratic elections, the e-voting system (or the simultaneous use of paper-ballot and e-voting methods) shall ensure equal suffrage. National legislation decides which of the multiple votes is counted. The "one person, one vote" principle must respected.

The decision on which vote is counted depends on the national policy towards remote voting. Countries that have a stricter policy towards remote voting will tend to give priority to the paper ballot if this is the vote issued at the polling station (controlled environment). Countries that are more open to remote voting may decide that the first validly issued vote is the one that counts, and in this case an e-vote from an uncontrolled environment may supersede a later-issued paper vote. Decisions on how to deal with voter coercion in the case of remote voting in general are to be taken by the national legislature. They should not be left to the e-voting administration alone, as they are a matter of remote voting policy in general, and not only of e-voting implementation.

- c. In all other cases appropriate measures should be taken to prevent a voter from casting more than one vote.

In countries where multiple voting is not allowed, multiple votes are considered as an attempt to cast more votes than a particular voter is permitted. This risk might arise, for instance, if the voter tries to cast multiple votes him or herself or if another person tries to use the voter's identity in order to vote, in the voter's name, after he or she has voted.

In the context of voting with paper ballots, this risk is managed through organisational measures. For instance, in the United Kingdom, if a person enters a polling station to vote and finds that somebody else has already voted in his or her name, that person is entitled to cast a special vote with a tendered ballot. This ballot is not placed in the ballot box but is sealed in an envelope, and is only looked at in the case of an election petition and in accordance with a direction of a court. A similar provision applies where two postal votes are received for the same voter. Appropriate measures need to be provided in the context of e-voting. Secure identification is important. Keeping the link between the voter's identification codes and his or her sealed ballot for a defined period may be one of the measures taken.

The introduction of remote e-voting brings with it the question of how the periods of time for voting in the polling station and remote e-voting are related. At first sight, it would seem logical that, for both methods of voting the same periods of time should apply, in order to avoid complications and distinctions. However, reasons that could lead to voting taking place at different times include:

- *when casting a vote in a polling station is the fall-back option for voters who are within the national territory in the event that the electronic voting channel breaks down, the closing time for the electronic voting channel has to be set before the closing time of the polling station;*
- *when the system is designed and operated in such a way that voters can choose between voting channels, but the channels used do not have access to a common register where the names of electors who have voted can be seen, the periods of time when these channels are available should generally not overlap.*

In all cases, counting should only start after the closure of all voting channels.

▸ d. In all cases, the voter should be clearly informed about the voting possibilities that are offered and about the rules for the counting of votes.

It is particularly important to inform the voter his or her voting possibilities, including the possibility to issue more than one e-vote or to vote more than once through different voting channels successively, where multiple voting is allowed.

In all cases the voter should be informed about the vote counting rules in force, in particular about which vote will finally be counted.

III. Guidelines for the implementation of free suffrage recommendations

10. The voter's intention shall not be affected by the voting system, or by any undue influence.

▸ a. In the case of remote e-voting, the voter should be informed about the means to verify that a connection to the official server has been established and that the authentic ballot has been presented.

In the context of remote e-voting, possible scenarios to be considered are that fraudulent servers may be introduced, for example imitating an official server by tampering with the domain name system (DNS), using a similar domain name to that of the official server, or corruption of the server code (for example, via malware), among others. Voters receive information on how to check the certificate of the official e-voting site. Electronic signatures applied to the ballot by the electoral authority allow for verification of the ballot. This, however, shall not violate the confidentiality of the vote.

▸ b. The e-voting system should not permit any manipulative influence to be exercised over the voter during the voting. In particular, the electronic ballot by which an electronic vote is cast should be free from any unofficial information.

Similar to provision 5a, this guideline requires that the voter be presented only with official voting information and that any manipulative influence from unauthorised parties be excluded.

▸ c. The e-voting system should introduce all possible measures to avoid any manipulative influence to be exercised over the vote once it has been cast, and it will include measures to allow verification that no such influence was exercised.

The concept of free suffrage also protects the vote from any manipulative influence after it has been cast. Any manipulative influence on or unauthorised intervention in the vote must be avoided. Of course, if authorised, multiple voting is not affected by this provision and the voter should be allowed to vote multiple times.

The provision aims at preventing any unauthorised changes to the vote, once it has been cast. It protects from attacks coming from outside the system and from internal threats. Individual and universal verifiability (see standards 15 and 17) are checks that aim at detecting any such unauthorised intervention.

▸ d. Where considered necessary, the e-voting system should offer mechanisms (for example, multiple voting) to protect voters from coercion to cast a vote in a specific way.

Multiple voting is considered to be a mechanism that protects the voter from coercers by allowing him or her to re-vote.

12. The way in which voters are guided through the e-voting process shall not lead them to vote precipitately or without confirmation.

▸ a. Voters should be able to alter their choice at any point in the remote e-voting process before casting their vote, or to break off the procedure.

This provision foresees the possibility of breaking off the procedure before the vote is cast, that is, before it enters the electronic ballot box. Once the vote is registered this will no longer be possible. The interface must therefore be programmed to attract voters' attention to this point, for instance by asking them to confirm their intentions before issuing the vote. It would be useful also to remind voters that this operation will validate and finalise the vote in cases where multiple voting is not allowed.

15. The voter shall be able to verify that his or her intention is accurately represented in the vote and that the sealed vote has entered the electronic ballot box without being altered. Any undue influence that has modified the vote shall be detectable.

▸ a. When using e-voting machines in polling stations, member States should consider the use of paper ballots as a second medium to store the vote for verification purposes.

Also known as the voter-verified paper audit trail (VVPAT), this method aims at ensuring free suffrage where the vote takes place on e-voting machines in controlled environments. If the e-solution applied in polling stations is a ballot scanner, a second medium is not necessary as the ballot in this case is by definition paper.

Other solutions for providing a second medium include, for instance, parts of the ballot sheet that can be torn away (for example, Chaum's scantegrity model) for individual verifiability. They may be very similar to VVPAT or take another form.

They should be made of paper, which is both unalterable and human legible/verifiable.

The validity of this second medium is to be assessed by national regulations that will also decide what to do in case of discrepancies between electronic results and those produced by the second medium.

- b. A mandatory count of votes in the second medium in a statistically meaningful number of randomly selected polling stations should be carried out in particular for e-voting machines and optical scanners.

Criteria such as the percentage of votes or the number of polling stations where the count takes place, their designation, etc. should be decided at national level. They should make sure that the overall aim of ensuring free elections is attained.

IV. Guidelines for the implementation of voting secrecy recommendations

19. E-voting shall be organised in such a way as to ensure that the secrecy of the vote is respected at all stages of the voting procedure.

- a. Voter register data should be clearly separated from voting components.

This provision applies more specifically when biometric techniques to identify the voter are used in polling stations in addition to using e-voting machines or scanners for voting. Separating the two components ensures vote secrecy.

Where votes and anonymised voter information are kept together, end-to-end encryption must protect this information.

21. The e-voting system and any authorised party shall protect authentication data so that unauthorised parties cannot misuse, intercept, modify or otherwise gain knowledge of this data.

- a. Authentication should use cryptographic mechanisms.

This provision requires state-of-the-art technical solutions to protect authentication data.

23. An e-voting system shall not provide the voter with proof of the content of the vote cast for use by third parties.

- a. Where paper proof of the electronic vote is provided to the voter in a controlled environment, the voter should not be allowed to show it to any other person, or take this proof outside of the polling station.

The e-voting should not provide proof of the content of the vote to the voter. Where this is programmed at some point in the voting procedure, as may be the case when voting on e-voting machines in polling stations, organisational measures should be in place to prevent any use of this proof to breach the secrecy

of the vote. The aim is to protect voting secrecy and prevent the practice of vote selling. Of course this does not prevent the voter, in absolute terms, from disclosing the content of his or her vote, for instance by taking a picture of it. It is up to the national criminal or administrative laws, which also apply to e-voting, to sanction such breaches of voting secrecy.

- b. No residual information related to the voter's decision should be displayed after the vote has been cast.

The term "residual information" refers to information that remains accessible at various locations (in the personal computer's memory, the browser cache, the video memory, swap files, temporary files, etc.) after the vote has been cast and which may reveal the voter's decision.

The provision advises the system developers or service providers to design the e-voting system in such a way that residual information is deleted after the vote has been cast. Technically there may be limited means to ensure this in a remote voting environment. Nevertheless, every measure possible should be taken to delete such residual information when the vote has been cast. However, individual verifiability can be implemented provided adequate safeguards exist to prevent coercion or vote-buying.

- c. In the case of remote e-voting, the voter should be informed of possible risks to voting secrecy and recommended means to reduce them ahead of voting.

- d. In the case of remote e-voting, the voter should be informed on how to delete, where it is possible, traces of the vote from the device used to cast the vote.

Guidelines 23c and 23d: In the case of remote e-voting, voters should be clearly informed of the risk of breach of secrecy of the vote and on measures and good practices to adopt to counter this risk, for instance by using firewalls, cleaning traces, etc. The system itself should delete automatically as many such traces as possible.

E-voting from a remote, uncontrolled environment implies shared responsibilities between the voter and the e-voting system/election administration body. It is part of the voter's responsibility to adopt the recommended measures (referred to in this provision). It is the duty of the electoral authority to clearly inform the voter on at least three points: the principle of shared responsibilities; the different measures to be adopted by the voter to reduce risk (running an anti-virus software, firewall, deleting traces of the vote, etc.); and remaining risks and verifiability techniques.

Such information should reach the voter well ahead of the voting period. Based on this, the voter can decide whether or not to use remote e-voting.

Warning messages may appear at the beginning of the e-voting procedure; a message on recommended steps that the voter should follow after voting (deleting traces, for instance) may need to be transmitted to the voter at the end of the e-voting procedure. However, such messages are only reminders and do not

replace the initial complete information that the voter should receive ahead of the e-voting period.

26. The e-voting process, in particular the counting stage, shall be organised in such a way that it is not possible to reconstruct a link between the unsealed vote and the voter. Votes are, and remain, anonymous.

- a. Voter information should be separated from the voter's decision at a pre-defined stage of the counting process.
- b. Any decoding required for the counting of the votes should be carried out as soon as practicable after the closure of the voting period.

The term "voter information" refers to anonymised information on the voter, such as the identification codes used in remote e-voting. Whereas the link between such information and the sealed vote must be maintained for a certain time under appropriate protection, to allow, in particular, the possibility of multiple voting while respecting the "one person, one vote" principle, the link should be destroyed before the counting takes place.

The encryption of votes will generally be necessary to secure the anonymity of voting. In many cases the vote is encrypted before starting the transmission via computer networks. It is held encrypted in the ballot box and is decoded before counting. The counting is carried out with decoded votes, which cannot be related to any voter.

However, there are encryption methods that do not require decoding before votes are counted (homomorphic encryption). Counting can then be performed without disclosing the content of encrypted votes. In some cases it may even be necessary for counting to be performed while votes are in the encrypted state, in order to secure anonymity.

- c. Member States should take the necessary steps to ensure that the confidentiality of any information obtained by any person while carrying out auditing functions is guaranteed.

In addition to protecting the information gathered by the audit system against unauthorised access, legal and organisational measures should be taken to check the persons that have authorised access to the audit system. Such measures could, for instance, be included in the accreditation process.

V. Guidelines for the implementation of regulatory and organisational recommendations

27. Member States that introduce e-voting shall do so in a gradual and progressive manner.

- a. A formal feasibility study should be undertaken and published before the selection and implementation of any e-voting technology. It should include reasons for the adoption of this system, risk analysis, an assessment

of the legal framework, the planning of pilots and the evaluation thereof, as well as a costbenefit analysis.

- b. Any implementation of e-voting pilots should start well ahead of elections and include essential preparations such as the adoption of detailed regulations, if necessary, for the pilots and system testing.

- c. The final version of the e-voting system should be tested before it is used in regular, binding elections.

- d. Pilots should be conducted on the basis of clear and comprehensive criteria to evaluate the effectiveness and integrity of the e-voting system, including the transmission of results.

28. Before introducing e-voting, member States shall introduce the required changes to the relevant legislation.

- a. The legal framework should include procedures for the implementation of e-voting from set-up and operation to counting.

  Detailed provisions will most probably appear in lower-level regulations and instructions. This should be provided for in higher-level laws which should also clarify the responsibilities for adopting such detailed regulations.

- b. The legal framework should include rules for determination of the validity of an electronic vote.

- c. The legal framework should include rules dealing with problems, failures and discrepancies resulting from the use of verification tools.

  When member States use a second medium to store the vote and a mandatory count is carried out, discrepancies between the results of votes cast may arise. In such cases the rules should make clear which type of vote (electronic or the alternative medium) takes precedence. An argument for the electronic vote is that voters have cast their vote in this manner. A case for the second medium would be that this vote could have been verified by the voter themselves, particularly if the medium under consideration includes a paper trail.

  Therefore in case of any discrepancy, the case should be examined thoroughly and any decision on the result of the vote count should depend on the result of the investigation. Member States are asked to establish rules which should address which vote is used in the official counts, if and when a recount is considered necessary, when and how the mandatory count takes place, under which circumstances all second votes are counted, and when a re-election should be held.

- d. The legal framework should include procedures for the process of data destruction, in particular to align processing, storing and destruction of the

data (and equipment) of voting technology with the personal data protection legislation.

The storage medium that contains the votes (hard drive, memory sticks, etc.) should be destroyed.

- e. The legal framework should include provisions for domestic and international observers.

Member States should include the role of domestic and international observers in the e-voting process and should regulate this in line with international commitments and good practice. The type of access to e-voting that observers will have will depend on national provisions. These should reflect international commitments, such as those of the Office for Democratic Institutions and Human Rights of the Organization for Security and Co-operation in Europe (OSCE/ODIHR). Observers should include representatives of political parties and the general public.

- f. Legislation should provide for clear timetables concerning all stages of the e-election.

An e-election can differ from an election or referendum with regard to the procedures that have to be followed by voters. Examples of potential differences are the period of time during which votes can be cast, the steps a voter has to take in order to participate in the e-election and the way the e-voting actually takes place. These differences should be clearly communicated to the voter in order to avoid any misunderstanding of the procedures and in order to give the voter all the information necessary to be able to make a well-founded decision on which voting channel to use. Careful consideration should be given to how much time the voter needs for this decision.

- g. The period in which an electronic vote can be cast should not begin before the notification of an election or a referendum.

Communicating the period of time for voting is especially important when the e-voting time period differs from other voting channels. This difference arises particularly in the case of remote e-voting in which a different period of time for voting using the electronic voting channels may be necessary, due to the specific nature of those channels.

- h. Remote e-voting may start and/or end at an earlier time than the opening of any polling station.

- i. The period in which an electronic vote can be cast should not continue after the end of the voting period.

Guidelines 28h and 28i: For various reasons, the period of remote e-voting may be longer than the period during which the polling stations are open. These reasons include providing a better service for citizens and enhancing accessibility.

However, remote e-voting should not continue after the end of the voting period at polling stations. In the case of the e-voting system being unavailable (for example, if a voter's personal computer is not working due to a power failure), a voter who is living or staying within the country where the election or referen-

dum takes place should still be able to go to the polling station to cast his or her vote. If e-voting were to continue after polling stations close, the voter would not have this possibility.

- j. The depositing of electronic votes into the electronic ballot box should be allowed for a sufficient period of time after the end of the e-voting period to allow for any delays in the passing of messages over the remote e-voting channel.

- k. After the end of the e-voting period, no voter should be allowed to gain access to the e-voting system.

Guidelines 28j and 28k: These provisions deal with internet voting sessions that start shortly before the e-voting channel closes. The ballot box should stay open to be able to collect these votes. The duration will be equivalent to the normal duration of an e-voting session to allow those voters who access the system a few seconds before it closes to finish the e-voting process normally.

Another case, again in internet voting scenarios, relates to a higher demand on the services which might occur in the short period just before the poll closes. This may lead to delays before the vote enters the electronic ballot box. Votes that have been sent in time should not be discarded as a result of such delays. The processing of the votes must not be shut down immediately after the closing of the e-voting service. However, starting an e-voting session after the system has closed should not be possible.

29. The relevant legislation shall regulate the responsibilities for the functioning of e-voting systems and ensure that the electoral management body has control over them.

- a. Procurement processes for e-voting should be carried out in a transparent manner.

- b. Provisions should be made to ensure against possible conflicts of interest of private stakeholders involved in the process.

- c. A strict separation of duties shall be maintained and documented.

- d. Member States should take appropriate measures to avoid circumstances where the election is unduly dependent on vendors.

30. Any observer shall be able to observe the count of the votes. The electoral management body shall be responsible for the counting process.

- a. A record of the counting process of the electronic votes should be kept, including information about the start and end of, and the persons involved in, the count.

- b. The counting of votes should be reproducible. There should be a possibility

to obtain sound evidence that the counting procedure has been performed satisfactorily including through an independent recount.

The objective here is that there should be a possibility to obtain sound evidence that the counting procedure has been performed correctly. An independent recount is one way to do this, if it is done with a different system from a different source. However, this can be achieved by other means, for example, using cryptographic proof (universal verifiability).

- c. Other features that may influence the accuracy of the results of the e-voting system should be verifiable.

Depending on the system used, there may be elements other than a recount that contribute to the accuracy of the result. The confirmation that all votes cast have been counted is an example.

In addition to verification tools, the percentage of votes cast by e-voting and the comparison of the results of e-voting with the results of voting by other channels shall be considered to establish the plausibility of the e-voting results and to validate their accuracy.

- d. The e-voting system should maintain the availability and integrity of the electronic ballot box and the output of the counting process as long as is required.

The information kept in the electronic ballot box must be protected as long as is necessary to allow for possible recounts or legal challenges or other legal requirements in the member State in question.

VI. Guidelines for the implementation of transparency and observation recommendations

31. Member States shall be transparent in all aspects of e-voting.

- a. The competent electoral authorities should publish an official list of the software used in an e-election. At the very least it should indicate the software used, the version, date of installation and a brief description.

Constant developments in information and communication technologies require frequent updates of hardware and software and regular adaptations to central systems and voting facilities used in a controlled environment (for example, voting machines). For e-voting to remain transparent, exact, full, up-to-date descriptions of the hardware and software components should be published, thus enabling interested groups to verify for themselves that the systems in use correspond to the ones certified by the competent authorities. The results of certification should be made available to the authorities, political parties and, depending on the legal provisions in force, citizens.

- b. Public access to the components of the e-voting system and information thereon, in particular documentation, source code and non-disclosure agreements, should be disclosed to the stakeholders and the public at large, well in advance of the election period.

When an electronic device/system yields binding results, the technical details that determine what and how to calculate can easily become just as important as an electoral law that defines polling stations' counting rules. To ensure public confidence through transparency, the voting software source code, the configuration as well as the list of all hardware and software components of the e-voting system should be part of the audit trail. Protocols of audited processes such as the installation and set-up procedure, the verification that the certified source code is the one used during the election, and the tallying process of the electronic ballot sheets should also be part of the audit trail. This should help member States to provide relevant documentation to voters and third parties, including national and international observers and the media.

The expression "well in advance" implies that clear time frames are set in national regulations for such disclosure and that the planned deadlines allow stakeholders to exercise their rights, react to such disclosures, and request changes. The electoral management body should have the time and possibility to react to such feedback, including by updating the system. Publishing such information twelve months before the vote may respect the "well in advance" criteria. Shorter time frames for last-minute changes might be necessary. However the main elements should be disclosed well in advance and not just shortly before the election.

▸ c. Deployment of electronic voting technologies should include the development of comprehensive, detailed, step-by-step guidelines including a procedural manual.

32. The public, in particular voters, shall be informed, well in advance of the start of voting, in clear and simple language, about:
- any steps a voter may have to take in order to participate and vote;
- the correct use and functioning of an e-voting system;
- the e-voting timetable, including all stages

▸ a. Support and guidance material on voting procedures should be made available to voters.

Support and guidance material on voting procedures should be in place regardless of the specific channel used. For each electronic voting channel used, such information should be available at least on the same electronic voting channel. In other words, a website with help information and e-mail facilities, at the minimum, should be in place when internet is the e-voting channel and a telephone hotline should be in place when voting by telephone s possible.

▸ b. In the case of remote e-voting, voter information material should also be available through a different, widely available communication channel.

Information on remote e-voting should be available also on a fall-back, different, widely available communication channel for situations when the remote e-voting channel is out of order. For example, a telephone hotline might be such an alternative communication channel for internet voting.

- c. Voters should be provided with an opportunity to practise before, and separately from, the moment of casting an electronic vote. In such a case, participants should have their attention drawn explicitly to the fact that they are not participating in a real election or referendum.

  Traditional voting methods are well tried and tested in member States and voters are familiar with the general rules that govern them. The introduction of e-voting challenges the voter. Such systems and the way they operate are less easy to understand. To maintain voter understanding and confidence, steps should be taken to present the system to voters. This effort may need to continue over time.

  To promote understanding and confidence in any (new) e-voting system, opportunities to practise using it should be provided before and separately from the moment of casting an electronic vote (for example, through demo systems or test elections). Special attention should be paid to categories of voters liable to have greater difficulties (for example, the elderly) and their specific needs.

33. The components of the e-voting system shall be disclosed for verification and certification purposes.

- a. E-voting systems should generate reliable and sufficiently detailed observation data so that election observation can be carried out. It should be possible to reliably determine the time at which an event generated observation data. The authenticity, availability and integrity of the data should be maintained.

- b. Domestic and international observers should have access to all relevant documentation on e-voting processes.

  Access to documentation, including minutes, certification, testing and audit reports, and detailed documentation explaining the operation of the system, is essential for domestic and international observers. Such observers include representatives of political parties and the general public. They should be invited to relevant meetings. Where possible, member States, the vendor or the certification body should provide information to all stakeholders, for example by posting relevant documents on the internet well in advance of the election period.

  Member States should develop procedures to define who has access to what and when. Such procedures should also be developed for domestic and international observers as well as for the media. Procedures for other stakeholders such as citizens, political parties and NGOs also need to be established. Open access should be the central theme In these procedures.

  Member States should make these requirements clear to potential vendors who should also understand that stakeholders, and specifically domestic and international observers, require access to certain documentation during the tender process. Non-disclosure agreements, which prevent observers from publishing assessments and the facts on which assessments are based would deprive all stakeholders – most importantly observers – of important information.

▸ c. Member States should make the relevant documentation available to observers, as far as practicable, in a language commonly used in international relations.

Relevant information required by domestic and international observers to carry out their work satisfactorily should be available in the official language, or languages, of the country concerned. Such information should, as far as possible, also be made available in one of the official languages of the Council of Europe (English and French). In particular, international observers require access to documentation in one of these languages.

▸ d. Member States should provide training programmes for domestic and international observer groups.

E-voting systems are not easily understandable for non-e-voting-experts. In order to improve stakeholders' understanding of the system in use, training is necessary, in particular for domestic, but also for international observers. It should provide basic and easy tools for use in observation work, including ways to check seals, read a voting machine print out and read an audit file.

▸ e. Domestic and international observers and the media should be able to observe the testing of the software and hardware.

Stakeholders, including accredited observer groups, should not only have access to documents, but should also be able to observe the verification of the e-voting devices and system. The observation of such tests and/or audits should not interfere with the election process. Therefore, such monitoring should only take place under guidance of those responsible for the organisation of elections. As already mentioned, such observers should include representatives of political parties and the general public. Furthermore, the people observing the tests and/or audits should attend a training session in advance. The process should be open enough to allow observers to have full insight into the operation of the system.

▸ f. Election observers should have access to all steps of the evaluation and certification process.

In the past twenty years, election observation has proven to be a successful method to ensure transparency and access to elections. With the emergence of electronic voting, the established methodologies for election observation need to be updated. To enable observers to observe the certification of electronic voting systems, the duration of election observation missions needs to be extended. It is crucial that none of the procedures necessary for certification of e-voting take place behind closed doors as this would raise suspicion.

Observers, including representatives of political parties and the general public, should be granted access to all relevant information during the entire duration of the certification process in order to carry out their duty. Observers, for their part, need to disclose the methodology they are going to apply.

VII. Guidelines for the implementation of accountability recommendations

36. Member States shall develop technical, evaluation and certification requirements and shall ascertain that they fully reflect the relevant legal and democratic principles. Member States shall keep the requirements up to date.

▸ a. Member States should establish the aims of certification and the certification methods.

When considering certification of on-site or remote e-voting systems, the first step is to clearly define the aims of and requirements for the certification procedure. When drafting these requirements, it is important to verify that they are in line with domestic legislation and international standards, including any appeals or complaint procedures relating to the conduct of elections. Although a detailed list of requirements might initially seem to be a good way to guarantee a proper certification analysis, a strict legal framework might generate paradoxical effects. For example, auditors would be subject to a high level of supervision, but vendors could customise their products to the limited goal of simply fulfilling the prescribed requirements of a given electoral administration. In these circumstances, vendors might not optimise the product and the electoral administration would be obliged by its own legal rules to accept a sub-optimal product. The use of a contract where the award criterion is quality and not price should help to avoid this trap.

Defining the aims, requirements in terms of software, operating system, hardware and e-voting process, and the scope and methods will contribute to the effectiveness of the certification process, the usability of the certification regime and the overall transparency of e-voting systems.

Certification of e-voting systems is not limited to the initial certification; it also includes procedures for de-certification and re-certification of software, operating systems, hardware and processes.

Sociopolitical factors may condition citizens' confidence and pose a major challenge. As such factors may also have a bearing on certification processes; member States should promote scientific research in this field, including an international exchange of relevant information.

A framework should be established that ensures all parties are aware of and have a good understanding of the system. Work should be done in accordance with established methodologies such as confirmation testing, component testing, performance testing and functional testing.

37. Before an e-voting system is introduced and at appropriate intervals thereafter, and in particular after any significant changes are made to the system, an independent and competent body shall evaluate the compliance of the e-voting system and of any information and communication technology (ICT) component with the technical requirements. This may take the form of formal certification or other appropriate control.

▸ a. Member States should determine the apportioning of costs entailed in the certification process. They should define the responsibility, including financial, of the certification body for the quality of their work.

Anybody authorised to participate in the certification of an e-voting system, including certifiers, evaluators and auditors, must be independent and qualified. The criteria, modalities and competent institutions involved in the selection of certification bodies should therefore be explicitly laid down in national legislation. Member States are responsible for drafting the rules and guidelines for the selection process.

These procedures need to be known and made public well in advance of the election day. This will facilitate the task of vendors and foster electors' trust in procedures. The number of certification bodies should not be limited; anybody who is independent and qualified should be eligible to perform the certification. Preference should be given to the use of a European public tender or consultation with a set of potential certifiers for the determination of qualified certifiers.

Member States should consider having the selection procedure carried out by internationally certified professional auditors. For example, CISA (Certified Information System Auditors), is a standard of achievement for those who audit, control, monitor and assess an organisation's information technology and business systems. Attention should be paid to the costs of such procedures. Another important factor is that the use of international certificates should not become an obstacle for member States to use a specific e-voting system or even make it impossible for countries to use a specific valid e-voting system.

Member States should make explicit from the outset which bodies are responsible for the costs of the certification procedure. They may decide that the entire cost, including formal certification, is to be borne by the vendors, which could lead to a greater involvement by the latter. Costs could also be the responsibility of the member State in question, and a third option is to share the costs. The costs of certification should under no circumstances compromise the independence, integrity and quality of the certification process. Whichever option is chosen, the member State should have sufficient funding available and the decision should be made public.

▸ b. Evaluation and certification bodies should have full access to all relevant information and should be allotted sufficient time to carry out the certification process ahead of the election.

Certification bodies should have access to information and data which is necessary and sufficient to perform their duties, namely to reach a conclusion regarding the voting system under inspection; they should have sufficient time to review all information and data. Citizens have the right to know what kind of information has not been considered necessary and sufficient to conduct the certification. Moreover, rules regarding the relationship between the vendor and the certifier, such as non-disclosure agreements (NDA) or other similar documents should be made public.

In some cases, such as early elections or the introduction of a new voting system, certification processes may take place only shortly before the elections open. This entails a risk of not having sufficient time to undertake a thorough certification procedure and this could, in turn, jeopardise the credibility of the election. Therefore, the certification procedure needs to be finished ahead of th elections, giving enough time to review the conclusions.

One solution to save time and money is to certify only the modified modules and the sequence of the modules for future certification, once an initial certification process has been carried out and the e-voting component has been certified. This can only be done if a difference is made between major changes (modifications) and minor changes to the e-voting system.

- c. The mandate of the evaluation and certification bodies should be re-confirmed regularly at prescribed intervals.

  Member States should develop procedures not only for the initial selection procedure, but also for follow-up procedures such as re-examination or reconfirmation of the mandate and withdrawal of the mandate. The mandate given to any certification body to certify an e-voting system should be valid only for a limited time. Tenders need to be made at regular intervals, and these tenders need to be public. It must be made clear whether the decision to entrust system certification to a specific, selected certification body may be taken by the vendor or whether this decision lies with the competent electoral authority.

- d. The conclusions reached in a certification report should be self-explanatory with the information contained in that report.

  The certification report should be self-explanatory, namely that its conclusions should only be based on the information it contains, enabling a third party to replicate the same research and thereby confirm that the conclusions of the certification report are valid.

- e. Member States should set and publish clear rules with regard to the disclosure of the final certification report and of all relevant documents, bearing in mind the importance of transparency.

  Member States should devise and publish procedures in which it is defined who has access to what information and when. Specific attention must be given to the needs of domestic and international observers and to those of the media. Also, procedures for other stakeholders, such as citizens, political parties, NGOs and, not least, election officials need to be established. Such procedural rules are essential in order to reinforce citizens' confidence in the security and reliability of e-voting systems and in the oversight role of the electoral authorities. Non-disclosure of all or part of the certification report or of all relevant documents should only be considered in exceptional circumstances.

  Special attention must be given to those components of the software that are relevant for the system's security. This could be done by including the testing of security in test plans in order for the reader to understand how security was tested. Labelling of all documents by member States and vendors may also be considered.

Vendors and even certifiers themselves might not agree with publication of some or most of the documentation of the e-voting system, as they wish to protect intellectual property rights. So as to avoid excessive secrecy during certification processes, potential vendors and certifiers should therefore be made aware, during the tender process, that stakeholders need to be granted access to specific documentation. NDAs which prevent observers from publishing assessments and the facts on which assessments are based make it very difficult to conduct a meaningful observation.

Finally, in order to oversee the certification process, or to compensate for any partial and incomplete disclosure of information to the public, member States may establish specific committees with experts, academics and/or politicians. For example, in Belgium, a college of experts is responsible for overseeing the entire electoral process for the competent legislative assembly.

39. The e-voting system shall be auditable. The audit system shall be open and comprehensive, and actively report on potential issues and threats.

▸ a. The audit system should record times, events and actions, including:

- all voting-related information, including the number of eligible voters, the number of votes cast, the number of valid and invalid votes, the counts and recounts, etc.;
- any attacks on the operation of the e-voting system and its communications infrastructure;
- system failures, malfunctions and other threats to the system.

Automated tools and system procedures should enable the data to be analysed and reported on in a fast and accurate manner, thus enabling rapid corrective action. The audit system should provide verifiable reports on:

- *cross-checks of data;*
- *system or network attacks;*
- *intrusion detection and reporting;*
- *data manipulation;*
- *fraud and fraud attempts.*

The audit system should maintain records of any attacks on the operation of the election or referendum system or its communications infrastructure. The system shall include a function that detects and reports attempts at hacking, intrusion or manipulation. Detection of attacks on the voting system shall be logged, reported and acted on immediately.

The audit system should log all counts and recounts, including all decisions made, actions taken or exceptions made during the counting process.

▸ b. The e-voting system should maintain reliable synchronised time sources.

The accuracy of the time source should be sufficient to maintain time marks for audit trails and observation data, as well as for maintaining the time limits for registration, nomination, voting or counting.

There may be different accuracy requirements for different users of the time source, such as different tolerances for the registration event and casting a vote. This may lead to multiple time sources or a single time source that provides the highest accuracy. The term "time mark" is used as an indication for marking the data. There are several means available, depending on the situation: secure time stamps might be needed for critical events, whereas continuous sequence numbers or preserving the sequence may be sufficient for log entries. Note that time stamps on votes may jeopardise the confidentiality of the vote. Careful consideration should therefore be given as to how and if they should be used in relation to ballots or votes.

- c. The conclusions drawn from the audit process should be taken into consideration in future e-elections.

VIII. Guidelines for the implementation of system reliability and security recommendations

40. The electoral management body shall be responsible for the respect for and compliance with all requirements even in the case of failures and attacks. The electoral management body shall be responsible for the availability, reliability, usability and security of the e-voting system.

- a. The availability of e-voting services to all voters during the entire e-voting process must be maintained.

An e-voting system should be protected against malfunction and breakdown. However, the possibility of a breakdown can never be entirely excluded. Procedures and alternative solutions for emergency cases should be foreseen.

- b. Voters should be promptly informed through appropriate means in case of interruption, suspension or restart of the electronic voting system.
- c. The voting system does not exclude eligible voters from casting their vote.
- d. The e-voting system should maintain the availability and integrity of the votes.

From the moment the vote is cast, no one should be able to read or change it or relate the vote to the voter who cast it. This is achieved by the process of sealing the ballot box, and where the ballot box is remote from the voter, by sealing the vote throughout its transmission from voter to ballot box. In some circumstances, sealing has to be done by encryption.

To seal any ballot box, physical and organisational measures are needed. These may include physically locking the box, and ensuring more than one person guards it. In the case of an electronic ballot box, additional measures are necessary, such as access controls, authorisation structures and firewalls.

A vote is sealed when its content has been subject to the measures that ensure that it cannot be read, changed or related to the voter who cast it.

Service level agreements (SLAs) usually lay down availability and failure rates. A certain level of service degradation may be acceptable during failure periods, for example when a server in a cluster breaks. In registration processes, even short periods of service disruptions or maintenance periods may be tolerable.

The system developers, however, take into account the possibility of denial of service attacks and should document the contingency reserve in system performance that has been designated. Independent penetration tests can reduce the probability of successful deliberate service disruption.

The services to be preserved in availability depend on the stage – pre-voting, voting, post-voting. In the pre-voting stage, nominations, the registration processes and services are to be available; in the voting stage, the voting processes and services; and in the post-voting stage, the counting and reporting processes and services. Auditing processes must be available in all stages. The pre-defined limits for SLAs, tolerable failure rates or service degradation may be different for the various stages or services, however.

- e. Technical and organisational measures should be taken to ensure that no data is permanently lost in the event of a breakdown or a fault affecting the e-voting system.

- f. Member States should consider usability throughout the development of security mechanisms.

Guidelines 40e and 40f: This does not suggest that every possible method of protection available must be used. In each case, a choice will have to be made as to the nature and extent of the protection measures to be applied. A proper balance shall be struck between different, equally important factors, for example between the all-important need for security and the advisability of having systems that are easily usable by voters. In such a case, usability must not override the need for high levels of security but may be a factor in determining which security measures should be adopted. Similar considerations might apply if a very small additional security benefit is only achievable at an excessively high usability cost.

- g. Regular checks should be performed to ensure that e-voting system components operate in accordance with the system's technical specifications and that its services are available.

- h. Key e-voting equipment should be located in a secure area and that area shall, throughout the election or referendum period, be guarded against any unauthorised interference or access.

- i. During the election or referendum period, a disaster recovery plan should be in place.

Guidelines 40h and 40i: For their security, central systems must be installed in secure, controlled locations. Physical access should be controlled and restricted. An alternative location should also be planned to be able to react after a physical disaster, with the appropriate equipment pre-reserved (disaster recovery planning).

The electoral authorities must define a specific service level before running the system. Based on the desired service level, a risk analysis should be made and scenarios established. These will imply procedures, backup arrangements, resource reservation and so on.

- j. It should be possible to check the state of protection of the voting equipment at any time. Those responsible for the equipment should use special monitoring procedures to ensure that during the polling period the voting equipment and its use satisfy requirements.
- k. Sufficient backup arrangements should be in place and be permanently available to ensure that voting proceeds smoothly. Any backup system should conform to the same standards and requirements as the original system.
- l. The staff concerned should be ready to intervene rapidly according to a procedure drawn up by the competent electoral authorities.

    i. Those responsible for operating the equipment should draw up a contingency procedure.

    ii. All technical operations should be subject to a formal control procedure. Any substantial changes to key equipment should be notified.

Guidelines 40j, 40k and 40l: An electronic voting system needs formalised procedures for monitoring its security and reliability and dealing with problems, and adequate resources for troubleshooting the infrastructure.

The electoral authorities should be made aware of all critical changes made to the system in order to anticipate any consequences and choose the appropriate policy to communicate such changes.

- m. Any data retained after the election or referendum period should be stored securely.

All election or referendum data that must be stored should be stored in a secure manner. This means several copies of data will be needed on several types of information support (hard disk, tapes, optical media such as DVD or microfiche, USB memory key and printout) and they should be stored in different locations.

41. Only persons authorised by the electoral management body shall have access to the central infrastructure, the servers and the election data. Appointments of persons authorised to deal with e-voting shall be clearly regulated.

- a. Appointed persons shall have restricted access to e-voting services, depending on their user identity or their user role. User authentication should

be effective before any action can be carried out. Separation of duties should be clear and strictly enforced through technical measures.

- b. While an electronic ballot box is open, any authorised intervention affecting the system should be carried out by teams of at least two people, be the subject of a report, be monitored by representatives of the electoral management body and any election observers.

- c. Any other critical technical activity should be carried out by teams of at least two people. The composition of the teams should be regularly changed. As far as possible, such activities should be carried out outside election periods. They should be the subject of a report.

42. Before any e-election takes place, the electoral management body shall satisfy itself that the e-voting system is genuine and operates correctly.

- a. Before each election, the equipment should be checked and approved in accordance with a protocol drawn up by the competent electoral authorities. The equipment should be checked to ensure that it complies with technical specifications. The findings should be submitted to the competent electoral authorities.

A clear distinction should be made between checking done on a regular basis after each election or referendum, and the checking done whenever the system is modified in any respect. In the first case, employees of the entity running the election or referendum system might do the checking. However in the second case an external body should do the checking, as the check is closer to being a certification procedure.

43. A procedure shall be established for regularly installing updated versions and corrections of all relevant software.

- a. Formal procedures should be developed for the deployment of software and voting technology configurations. Deadlines for updates should be established. Updates that are distributed should be authenticated (signed).

46. The electoral management body shall handle all cryptographic material securely.

- a. The private cryptographic keys be should be generated at a public meeting and should be divided in separate parts and shared by at least two people who are unlikely to collude.

47. Where incidents that could threaten the integrity of the system occur, those responsible for operating the equipment shall immediately inform the electoral management body.

- a. The types of incidents are specified in advance by the electoral authorities.

▸ b. In case of an incident, competent electoral authorities should take the necessary steps to mitigate the effects of the incident.

48. The authenticity, availability and integrity of the voters' registers and lists of candidates shall be maintained. The source of the data shall be authenticated. Provisions on data protection shall be respected.

▸ a. Printing of voter identification data such as polling cards should be reviewed to ensure security of sensitive data.

49. The e-voting system shall identify votes that are affected by an irregularity.

▸ a. The fact that a vote has been cast within the prescribed time limits should be ascertainable.

In an internet voting context, the expression "within prescribed time limits" refers to the time limit where the internet voting channel closes. This can be implemented by using time marks or a confirmation of a trustworthy system. A time mark attached to the vote should not, however, be used to reveal the vote.

APPENDIX

DEFINITIONS

In these guidelines the following terms are used with the following meanings:

- access control: the prevention of unauthorised use of a resource;
- assessment: an evaluation of persons, hardware, software and procedures to verify if they are suitable for the fulfilment of certain tasks;
- audit: an independent pre- or post-election evaluation of a person, organisation, system, process, entity, project or product which includes quantitative and qualitative analysis;
- authentication: the provision of assurance of the claimed identity of a person or data;
- availability: the state of being accessible and usable upon demand;
- ballot: the legally recognised means by which the voter can express his or her vote;
- candidate: a voting option consisting of a person, a group of persons and/or a political party;
- casting of the vote: entering the vote in the ballot box;
- certificate: a document which is the result of a formal certification wherein a fact is certified or attested;

- certification: a process of confirmation that an e-voting system is in compliance with prescribed requirements and standards and that it includes, at the minimum, provisions to ascertain the correct functioning of the system. This can be done through measures ranging from testing and auditing through to formal certification. The end result is a report and/or a certificate;

- certification body (or certifier): an organisation entitled to conduct a certification process and to issue a certificate upon completion of the process;

- certification report: a document which explains what a certificate has certified and how it is certified;

- chain of trust: a process in computer security which is established by validating each component of hardware and software from the bottom up. It is intended to ensure that only trusted software and hardware can be used while still remaining flexible;

- component testing: a method by which individual units of the system code are tested to determine if they are fit for use;

- confidentiality: the state characterising information that should not be made available or disclosed to unauthorised individuals, entities or processes;

- controlled environment: premises supervised by election officials, e.g. polling stations, embassies or consulates;

- e-election: a political election or referendum where e-voting is used;

- electoral management body (EMB): institution in charge of managing elections in a given country at national or lower level;

- electronic ballot box: the electronic means by which the votes are stored pending being counted;

- e-vote: electronically cast vote;

- e-voting: the use of electronic means to cast and/or count the vote;

- e-voting system: the hardware, software and processes which allow voters to vote by electronic means in an election or referendum;

- formal certification: certification carried out by official authorities, only before election day and leading to the issuance of a certificate;

- guidelines: any document that aims to streamline particular processes according to a set routine. By definition, guidelines are not legally binding;

- non-disclosure agreement (NDA): a legal contract between at least two parties that outlines confidential material, knowledge, or information that the parties wish to share with one another for certain purposes, but wish to restrict access to by third parties;
- open access: access online to material that is free for all to read, and possibly to use (or reuse) within certain limits;
- protection profile: an implementation-independent set of security requirements for a category of products that meet the specific security needs of consumers;
- requirement: a singular documented need of what a particular product or service should be or perform;
- remote e-voting: the use of electronic means to cast the vote outside the premises where voting takes place in general;
- sealing: protecting information so that it cannot be used or interpreted without the help of other information or means available only to specific persons or authorities including through encryption;
- stakeholder: a person, group, organisation, or system that affects, or can be affected by, a government's or organisation's actions. These include citizens, election officials, political parties, governments, domestic and international observers, media, academics, (I)NGOs, anti-e-voting organisations and specific e-voting certification bodies;
- standard (legal): refers to provisions contained in the Appendix I to Recommendation CM/Rec(2017)5;
- standard (technical): an established norm usually in the form of a formal document that establishes uniform engineering or technical criteria, methods, processes and practices;
- testing: the process of verifying that the system works as expected;
- vote: the expression of the choice of voting option;
- voter: a person who is entitled to cast a vote in a particular election or referendum;
- voting channel: the way by which the voter can cast a vote;
- voting options: the range of possibilities from which a choice can be made through the casting of the vote in an election or referendum;
- voters' register: a list of persons entitled to vote (electors).

Declaration Decl (13/02/2019)1[1]

of the Committee of Ministers of the Council of Europe on the manipulative capabilities of algorithmic processes

Adopted by the Committee of Ministers of the Council of Europe on 13 February 2019 at the 1337th meeting of the Ministers' Deputies

1. Council of Europe member States have committed themselves to building societies based on the values of democracy, human rights and the rule of law. This commitment remains and should be honoured throughout the ongoing process of societal transformation that is fuelled by technological advancements. Member States must ensure the rights and freedoms enshrined in the Convention for the Protection of Human Rights and Fundamental Freedoms (ETS No. 5) to everyone within their jurisdiction, equally offline and online, in an environment of unprecedented political, economic and cultural globalisation and connectedness.

2. Digital services are used today as an essential tool of modern communication, including political communication between governments and between public institutions and citizens. Moreover, they are fundamental for a growing number of users for news consumption, education, entertainment, commercial transactions and multiple other forms of everyday activities. This results in unprecedented amounts of new data that are constantly created with mounting speed and scale.

3. Advanced technologies play a pivotal role in maintaining the efficiency and public service value of digitisation, in strengthening individual autonomy and self-determination, and in enhancing human flourishing by creating optimal conditions for the exercise of human rights. Reference is made in this context to Recommendation CM/Rec(2007)16 of the Committee of Ministers to member States on measures to promote the public service value of the internet; Recommendation CM/Rec(2014)6 of the Committee of Ministers to member States on a Guide to human rights for internet users; and Recommendation CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries.

4. Technology is an ever growing presence in our daily lives and prompts users to disclose their relevant, including personal, data voluntarily and for compara-

1. Source: www.coe.int/cm

tively small awards of personal convenience. Public awareness, however, remains limited regarding the extent to which everyday devices collect and generate vast amounts of data. These data are used to train machine-learning technologies to prioritise search results, to predict and shape personal preferences, to alter information flows, and, sometimes, to subject individuals to behavioural experimentation.

5. Current discussions regarding the application and strengthening of data protection laws should consider the particular risks for and interests of those persons that may be especially unaware of the dangers of data exploitation. This includes children as well as persons belonging to marginalised communities who may face language barriers or other structural disadvantages. It may also include those who, because of their particularly large digital footprint, are especially exposed to new forms of data-driven surveillance.

6. Increasingly, computational means make it possible to infer intimate and detailed information about individuals from readily available data. This supports the sorting of individuals into categories, thereby reinforcing different forms of social, cultural, religious, legal and economic segregation and discrimination. It also facilitates the micro-targeting of individuals based on profiles in ways that may profoundly affect their lives.

7. Moreover, data-driven technologies and systems are designed to continuously achieve optimum solutions within the given parameters specified by their developers. When operating at scale, such optimisation processes inevitably prioritise certain values over others, thereby shaping the contexts and environments in which individuals, users and non-users alike, process information and make their decisions. This reconfiguration of environments may be beneficial for some individuals and groups while detrimental to others, which raises serious questions about the resulting distributional outcomes. The effects of the targeted use of constantly expanding volumes of aggregated data on the exercise of human rights in a broader sense, significantly beyond the current notions of personal data protection and privacy, remain understudied and require serious consideration.

8. Contemporary machine learning tools have the growing capacity not only to predict choices but also to influence emotions and thoughts and alter an anticipated course of action, sometimes subliminally. The dangers for democratic societies that emanate from the possibility to employ such capacity to manipulate and control not only economic choices but also social and political behaviours, have only recently become apparent. In this context, particular attention should be paid to the significant power that technological advancement confers to those – be they public entities or private actors – who may use such algorithmic tools without adequate democratic oversight or control.

9. Fine grained, sub-conscious and personalised levels of algorithmic persuasion may have significant effects on the cognitive autonomy of individuals and their right to form opinions and take independent decisions. These effects remain

underexplored but cannot be underestimated. Not only may they weaken the exercise and enjoyment of individual human rights, but they may lead to the corrosion of the very foundation of the Council of Europe. Its central pillars of human rights, democracy and the rule of law are grounded on the fundamental belief in the equality and dignity of all humans as independent moral agents.

In view of the foregoing, the Committee of Ministers:

- draws attention to the growing threat to the right of human beings to form opinions and take decisions independently of automated systems, which emanates from advanced digital technologies. Attention should be paid particularly to their capacity to use personal and non-personal data to sort and micro-target people, to identify individual vulnerabilities and exploit accurate predictive knowledge, and to reconfigure social environments in order to meet specific goals and vested interests;

- encourages member States to assume their responsibility to address this threat by

  - a. ensuring that adequate priority attention is paid at senior level to this inter-disciplinary concern that often falls in between established mandates of relevant authorities;

  - b. considering the need for additional protective frameworks related to data that go beyond current notions of personal data protection and privacy and address the significant impacts of the targeted use of data on societies and on the exercise of human rights more broadly;

  - c. initiating, within appropriate institutional frameworks, open-ended, informed and inclusive public debates with a view to providing guidance on where to draw the line between forms of permissible persuasion and unacceptable manipulation. The latter may take the form of influence that is subliminal, exploits existing vulnerabilities or cognitive biases, and/or encroaches on the independence and authenticity of individual decision-making;

  - d. taking appropriate and proportionate measures to ensure that effective legal guarantees are in place against such forms of illegitimate interference; and

  - e. empowering users by promoting critical digital literacy skills and robustly enhancing public awareness of how many data are generated and processed by personal devices, networks, and platforms through algorithmic processes that are trained for data exploitation. Specifically, public awareness should be enhanced of the fact that algorithmic tools are widely used for commercial purposes and, increasingly, for political reasons, as well as for ambitions of anti- or undemocratic power gain, warfare, or to inflict direct harm;

- underlines equally the responsibility of member States to lead and support the exploration and research into the autonomy, equality and welfare enhancing potential of advanced data processing and machine learning technologies. In particular should incentives be created to develop services that strengthen equal access to and enjoyment of human rights, and create broad value for society, among others by encouraging the catering to the needs of historically marginalised or thus far underserved communities. To this end, structural diversity in innovation and research should be promoted;

- acknowledges the need to consider, at both national and international levels, the growing onus on the industry across sectors to live up to their important functions and influence with commensurate levels of increased fairness, transparency and accountability, in line with their responsibility to respect human rights and fundamental freedoms, and under the guidance of public institutions;

- stresses the societal role of academia in producing independent, evidence-based and interdisciplinary research and advice for decision-makers regarding the capacity of algorithmic tools to enhance or interfere with the cognitive sovereignty of individuals. This research should take account of existing diversity in societies, and should include all backgrounds and ages of users not only regarding their behaviours as consumers but including wider impacts on their emotional well-being and personal choices in societal, institutional and political contexts;

- draws attention to the necessity of critically assessing the need for stronger regulatory or other measures to ensure adequate and democratically legitimated oversight over the design, development, deployment and use of algorithmic tools, with a view to ensuring that there is effective protection against unfair practices or abuse of position of market power;

- emphasises in particular the need to assess the regulatory frameworks related to political communication and electoral processes to safeguard the fairness and integrity of elections offline as well as online in line with established principles. In particular it should be ensured that voters have access to comparable levels of information across the political spectrum, that voters are aware of the dangers of political redlining, which occurs when political campaigning is limited to those most likely to be influenced, and that voters are protected effectively against unfair practices and manipulation;

- underlines the vital role played by independent and pluralistic media in overseeing public affairs and processes on behalf of the electorate, thereby acting as public watchdogs and contributing to meaningful and informed debate;

- encourages member States to maintain an open and inclusive dialogue with all relevant stakeholders globally with a view to avoiding path dependencies and fully considering all available options towards effectively addressing this emerging and thus far understudied, and possibly underestimated, concern.

Modernised Convention[1]
for the Protection of Individuals with Regard to the Processing of Personal Data (Convention 108+)

Consolidated text [2]

Strasbourg, 28/01/1981 **– Convention for the Protection of Individuals with Regard to the Processing of Persondal Data (Treaty ETS No. 108) open for signature by the Council of Europe member States and for accession by non-member States**

Strasbourg, 08/11/2001 **– Treaty, as amended by Additional Protocol (ETS No. 181), open for signature by the Signatories of the Treaty ETS No. 108 and by the European Union, and for accession by the States having acceded to Treaty ETS No. 108**

Strasbourg, 10/10/2018 **– Treaty, as amended by Protocol (CETS No. 223), open for signature by the Contracting States to Treaty ETS No. 108**

PREAMBLE

The member States of the Council of Europe, and the other signatories hereto,

Considering that the aim of the Council of Europe is to achieve greater unity between its members, based in particular on respect for the rule of law, as well as human rights and fundamental freedoms;

Considering that it is necessary to secure the human dignity and protection of the human rights and fundamental freedoms of every individual and, given the diversification, intensification and globalisation of data processing and personal data flows, personal autonomy based on a person's right to control of his or her personal data and the processing of such data;

Recalling that the right to protection of personal data is to be considered in respect of its role in society and that it has to be reconciled with other human rights and fundamental freedoms, including freedom of expression;

Considering that this Convention permits account to be taken, in the implementation of the rules laid down therein, of the principle of the right of access to official documents;

Recognising that it is necessary to promote at the global level the fundamental values of respect for privacy and protection of personal data, thereby contributing to the free flow of information between people;

Recognising the interest of a reinforcement of international co-operation between the Parties to the Convention,

---

1. Source: Treaty Office on conventions.coe.int.
2. Convention for the Protection of Individuals with regard to Automatic Processing of Pesonal Data as it will be amended by its protocol CETS No.223 upon its entry into force.

Have agreed as follows:

CHAPTER I – GENERAL PROVISIONS

Article 1 – Object and purpose

The purpose of this Convention is to protect every individual, whatever his or her nationality or residence, with regard to the processing of their personal data, thereby contributing to respect for his or her human rights and fundamental freedoms, and in particular the right to privacy.

Article 2 – Definitions

For the purposes of this Convention:

- a. "personal data" means any information relating to an identified or identifiable individual ("data subject");
- b. "data processing" means any operation or set of operations performed on personal data, such as the collection, storage, preservation, alteration, retrieval, disclosure, making available, erasure, or destruction of, or the carrying out of logical and/or arithmetical operations on such data;
- c. Where automated processing is not used, "data processing" means an operation or set of operations performed upon personal data within a structured set of such data which are accessible or retrievable according to specific criteria;
- d. "controller" means the natural or legal person, public authority, service, agency or any other body which, alone or jointly with others, has decision-making power with respect to data processing;
- e. "recipient" means a natural or legal person, public authority, service, agency or any other body to whom data are disclosed or made available;
- f. "processor" means a natural or legal person, public authority, service, agency or any other body which processes personal data on behalf of the controller.

Article 3 – Scope

1. Each Party undertakes to apply this Convention to data processing subject to its jurisdiction in the public and private sectors, thereby securing every individual's right to protection of his or her personal data.
2. This Convention shall not apply to data processing carried out by an individual in the course of purely personal or household activities.

CHAPTER II – BASIC PRINCIPLES FOR THE PROTECTION OF PERSONAL DATA

Article 4 – Duties of the Parties

1. Each Party shall take the necessary measures in its law to give effect to the provisions of this Convention and secure their effective application.
2. These measures shall be taken by each Party and shall have come into force by the time of ratification or of accession to this Convention.

3. Each Party undertakes:

   - a. to allow the Convention Committee provided for in Chapter VI to evaluate the effectiveness of the measures it has taken in its law to give effect to the provisions of this Convention; and

   - b. to contribute actively to this evaluation process.

Article 5 – Legitimacy of data processing and quality of data

1. Data processing shall be proportionate in relation to the legitimate purpose pursued and reflect at all stages of the processing a fair balance between all interests concerned, whether public or private, and the rights and freedoms at stake.

2. Each Party shall provide that data processing can be carried out on the basis of the free, specific, informed and unambiguous consent of the data subject or of some other legitimate basis laid down by law.

3. Personal data undergoing processing shall be processed lawfully.

4. Personal data undergoing processing shall be:

   - a. processed fairly and in a transparent manner;

   - b. collected for explicit, specified and legitimate purposes and not processed in a way incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is, subject to appropriate safeguards, compatible with those purposes;

   - c. adequate, relevant and not excessive in relation to the purposes for which they are processed;

   - d. accurate and, where necessary, kept up to date;

   - e. preserved in a form which permits identification of data subjects for no longer than is necessary for the purposes for which those data are processed.

Article 6 – Special categories of data

1. The processing of:

   - genetic data;
   - personal data relating to offences, criminal proceedings and convictions, and related security measures;
   - biometric data uniquely identifying a person;

- personal data for the information they reveal relating to racial or ethnic origin, political opinions, trade-union membership, religious or other beliefs, health or sexual life,

shall only be allowed where appropriate safeguards are enshrined in law, complementing those of this Convention.

2. Such safeguards shall guard against the risks that the processing of sensitive data may present for the interests, rights and fundamental freedoms of the data subject, notably a risk of discrimination.

Article 7 – Data security

1. Each Party shall provide that the controller, and, where applicable the processor, takes appropriate security measures against risks such as accidental or unauthorised access to, destruction, loss, use, modification or disclosure of personal data.

2. Each Party shall provide that the controller notifies, without delay, at least the competent supervisory authority within the meaning of Article 15 of this Convention, of those data breaches which may seriously interfere with the rights and fundamental freedoms of data subjects.

Article 8 – Transparency of processing

1. Each Party shall provide that the controller informs the data subjects of:

   - a. his or her identity and habitual residence or establishment;
   - b. the legal basis and the purposes of the intended processing;
   - c. the categories of personal data processed;
   - d. the recipients or categories of recipients of the personal data, if any; and
   - e. the means of exercising the rights set out in Article 9,

   as well as any necessary additional information in order to ensure fair and transparent processing of the personal data.

2. Paragraph 1 shall not apply where the data subject already has the relevant information.

3. Where the personal data are not collected from the data subjects, the controller shall not be required to provide such information where the processing is expressly prescribed by law or this proves to be impossible or involves disproportionate efforts.

Article 9 – Rights of the data subject

1. Every individual shall have a right:

   - a. not to be subject to a decision significantly affecting him or her based solely on an automated processing of data without having his or her views taken into consideration;

- b. to obtain, on request, at reasonable intervals and without excessive delay or expense, confirmation of the processing of personal data relating to him or her, the communication in an intelligible form of the data processed, all available information on their origin, on the preservation period as well as any other information that the controller is required to provide in order to ensure the transparency of processing in accordance with Article 8, paragraph 1;

- c. to obtain, on request, knowledge of the reasoning underlying data processing where the results of such processing are applied to him or her;

- d. to object at any time, on grounds relating to his or her situation, to the processing of personal data concerning him or her unless the controller demonstrates legitimate grounds for the processing which override his or her interests or rights and fundamental freedoms;

- e. to obtain, on request, free of charge and without excessive delay, rectification or erasure, as the case may be, of such data if these are being, or have been, processed contrary to the provisions of this Convention;

- f. to have a remedy under Article 12 where his or her rights under this Convention have been violated;

- g. to benefit, whatever his or her nationality or residence, from the assistance of a supervisory authority within the meaning of Article 15, in exercising his or her rights under this Convention.

2. Paragraph 1.a shall not apply if the decision is authorised by a law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights, freedoms and legitimate interests.

Article 10 – Additional obligations

1. Each Party shall provide that controllers and, where applicable, processors, take all appropriate measures to comply with the obligations of this Convention and be able to demonstrate, subject to the domestic legislation adopted in accordance with Article 11, paragraph 3, in particular to the competent supervisory authority provided for in Article 15, that the data processing under their control is in compliance with the provisions of this Convention.

2. Each Party shall provide that controllers and, where applicable, processors, examine the likely impact of intended data processing on the rights and fundamental freedoms of data subjects prior to the commencement of such processing, and shall design the data processing in such a manner as to prevent or minimise the risk of interference with those rights and fundamental freedoms.

3. Each Party shall provide that controllers, and, where applicable, processors, implement technical and organisational measures which take into account the implications of the right to the protection of personal data at all stages of the data processing.

4. Each Party may, having regard to the risks arising for the interests, rights and fundamental freedoms of the data subjects, adapt the application of the provisions of paragraphs 1, 2 and 3 in the law giving effect to the provisions of this Convention, according to the nature and volume of the data, the nature, scope and purpose of the processing and, where appropriate, the size of the controller or processor.

Article 11 – Exceptions and restrictions

1. No exception to the provisions set out in this Chapter shall be allowed except to the provisions of Article 5 paragraph 4, Article 7 paragraph 2, Article 8 paragraph 1 and Article 9, when such an exception is provided for by law, respects the essence of the fundamental rights and freedoms and constitutes a necessary and proportionate measure in a democratic society for:

   - a. the protection of national security, defense, public safety, important economic and financial interests of the State, the impartiality and independence of the judiciary or the prevention, investigation and prosecution of criminal offences and the execution of criminal penalties, and other essential objectives of general public interest;

   - b. the protection of the data subject or the rights and fundamental freedoms of others, notably freedom of expression.

2. Restrictions on the exercise of the provisions specified in Articles 8 and 9 may be provided for by law with respect to data processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes when there is no recognisable risk of infringement of the rights and fundamental freedoms of data subjects.

3. In addition to the exceptions allowed for in paragraph 1 of this article, with reference to processing activities for national security and defense purposes, each Party may provide, by law and only to the extent that it constitutes a necessary and proportionate measure in a democratic society to fulfill such aim, exceptions to Article 4 paragraph 3, Article 14 paragraphs 5 and 6 and Article 15, paragraph 2, litterae a, b, c and d.

This is without prejudice to the requirement that processing activities for national security and defense purposes are subject to independent and effective review and supervision under the domestic legislation of the respective Party.

Article 12 – Sanctions and remedies

Each Party undertakes to establish appropriate judicial and non-judicial sanctions and remedies for violations of the provisions of this Convention.

Article 13 – Extended protection

None of the provisions of this chapter shall be interpreted as limiting or otherwise affecting the possibility for a Party to grant data subjects a wider measure of protection than that stipulated in this Convention.

CHAPTER III – TRANSBORDER FLOWS OF PERSONAL DATA

Article 14 – Transborder flows of personal data

1. A Party shall not, for the sole purpose of the protection of personal data, prohibit or subject to special authorisation the transfer of such data to a recipient who is subject to the jurisdiction of another Party to the Convention. Such a Party may, however, do so if there is a real and serious risk that the transfer to another Party, or from that other Party to a non-Party, would lead to circumventing the provisions of the Convention. A Party may also do so, if bound by harmonised rules of protection shared by States belonging to a regional international organisation.

2. When the recipient is subject to the jurisdiction of a State or international organisation which is not Party to this Convention, the transfer of personal data may only take place where an appropriate level of protection based on the provisions of this Convention is secured.

3. An appropriate level of protection can be secured by:

   - a. the law of that State or international organisation, including the applicable international treaties or agreements; or

   - b. ad hoc or approved standardised safeguards provided by legally-binding and enforceable instruments adopted and implemented by the persons involved in the transfer and further processing.

4. Notwithstanding the provisions of the previous paragraphs, each Party may provide that the transfer of personal data may take place if:

   - a. the data subject has given explicit, specific and free consent, after being informed of risks arising in the absence of appropriate safeguards; or

   - b. the specific interests of the data subject require it in the particular case; or

   - c. prevailing legitimate interests, in particular important public interests, are provided for by law and such transfer constitutes a necessary and proportionate measure in a democratic society; or

   - d. it constitutes a necessary and proportionate measure in a democratic society for freedom of expression.

5. Each Party shall provide that the competent supervisory authority within the

meaning of Article 15 of this Convention is provided with all relevant information concerning the transfers of data referred to in paragraph 3.b and, upon request, paragraphs 4.b and 4.c.

6. Each Party shall also provide that the supervisory authority is entitled to request that the person who transfers data demonstrates the effectiveness of the safeguards or the existence of prevailing legitimate interests and that the supervisory authority may, in order to protect the rights and fundamental freedoms of data subjects, prohibit such transfers, suspend them or subject them to condition.

CHAPTER IV – SUPERVISORY AUTHORITIES

Article 15 – Supervisory authorities

1. Each Party shall provide for one or more authorities to be responsible for ensuring compliance with the provisions of this Convention.

2. To this end, such authorities:

   - a. shall have powers of investigation and intervention;
   - b. shall perform the functions relating to transfers of data provided for under Article 14, notably the approval of standardised safeguards;
   - c. shall have powers to issue decisions with respect to violations of the provisions of this Convention and may, in particular, impose administrative sanctions;
   - d. shall have the power to engage in legal proceedings or to bring to the attention of the competent judicial authorities violations of the provisions of this Convention;
   - e. shall promote:

     i. public awareness of their functions and powers as well as their activities;

     ii. public awareness of the rights of data subjects and the exercise of such rights;

     iii. awareness of controllers and processors of their responsibilities under this Convention;

     specific attention shall be given to the data protection rights of children and other vulnerable individuals.

3. The competent supervisory authorities shall be consulted on proposals for any legislative or administrative measures which provide for the processing of personal data.

4. Each competent supervisory authority shall deal with requests and complaints lodged by data subjects concerning their data protection rights and shall keep data subjects informed of progress.

5. The supervisory authorities shall act with complete independence and

impartiality in performing their duties and exercising their powers and in doing so shall neither seek nor accept instructions.

6. Each Party shall ensure that the supervisory authorities are provided with the resources necessary for the effective performance of their functions and exercise of their powers.

7. Each supervisory authority shall prepare and publish a periodical report outlining its activities.

8. Members and staff of the supervisory authorities shall be bound by obligations of confidentiality with regard to confidential information to which they have access, or have had access to, in the performance of their duties and exercise of their powers.

9. Decisions of the supervisory authorities may be subject to appeal through the courts.

10. The supervisory authorities shall not be competent with respect to processing carried out by bodies when acting in their judicial capacity.

CHAPTER V – CO-OPERATION AND MUTUAL ASSISTANCE

Article 16 – Designation of supervisory authorities

1. The Parties agree to co-operate and render each other mutual assistance in order to implement this Convention.

2. For that purpose:

   - a. each Party shall designate one or more supervisory authorities within the meaning of Article 15 of this Convention, the name and address of each of which it shall communicate to the Secretary General of the Council of Europe;

   - b. each Party which has designated more than one supervisory authority shall specify the competence of each authority in its communication referred to in the previous littera.

Article 17 – Forms of co-operation

1. The supervisory authorities shall co-operate with one another to the extent necessary for the performance of their duties and exercise of their powers, in particular by:

   - a. providing mutual assistance by exchanging relevant and useful information and co-operating with each other under the condition that, as regards the protection of personal data, all the rules and safeguards of this Convention are complied with;

- b. co-ordinating their investigations or interventions, or conducting joint actions;
- c. providing information and documentation on their law and administrative practice relating to data protection.

2. The information referred to in paragraph 1 shall not include personal data undergoing processing unless such data are essential for co-operation, or where the data subject concerned has given explicit, specific, free and informed consent to its provision.

3. In order to organise their co-operation and to perform the duties set out in the preceding paragraphs, the supervisory authorities of the Parties shall form a network.

Article 18 – Assistance to data subjects

1. Each Party shall assist any data subject, whatever his or her nationality or residence, to exercise his or her rights under Article 9 of this Convention.

2. Where a data subject resides on the territory of another Party, he or she shall be given the option of submitting the request through the intermediary of the supervisory authority designated by that Party.

3. The request for assistance shall contain all the necessary particulars, relating inter alia to:

- a. the name, address and any other relevant particulars identifying the data subject making the request;
- b. the processing to which the request pertains, or its controller;
- c. the purpose of the request.

Article 19 – Safeguards

1. A supervisory authority which has received information from another supervisory authority, either accompanying a request or in reply to its own request, shall not use that information for purposes other than those specified in the request.

2. In no case may a supervisory authority be allowed to make a request on behalf of a data subject of its own accord and without the express approval of the data subject concerned.

Article 20 – Refusal of requests

A supervisory authority to which a request is addressed under Article 17 of this Convention may not refuse to comply with it unless:

- a. the request is not compatible with its powers;
- b. the request does not comply with the provisions of this Convention;

- c. compliance with the request would be incompatible with the sovereignty, national security or public order of the Party by which it was designated, or with the rights and fundamental freedoms of individuals under the jurisdiction of that Party.

Article 21 – Costs and procedures

1. Co-operation and mutual assistance which the Parties render each other under Article 17 and assistance they render to data subjects under Articles 9 and 18 shall not give rise to the payment of any costs or fees other than those incurred for experts and interpreters. The latter costs or fees shall be borne by the Party making the request.

2. The data subject may not be charged costs or fees in connection with the steps taken on his or her behalf in the territory of another Party other than those lawfully payable by residents of that Party.

3. Other details concerning the co-operation and assistance, relating in particular to the forms and procedures and the languages to be used, shall be established directly between the Parties concerned.

CHAPTER VI – CONVENTION COMMITTEE

Article 22 – Composition of the committee

1. A Convention Committee shall be set up after the entry into force of this Convention.

2. Each Party shall appoint a representative to the committee and a deputy representative. Any member State of the Council of Europe which is not a Party to the Convention shall have the right to be represented on the committee by an observer.

3. The Convention Committee may, by a decision taken by a majority of two-thirds of the representatives of the Parties, invite an observer to be represented at its meetings.

4. Any Party which is not a member of the Council of Europe shall contribute to the funding of the activities of the Convention Committee according to the modalities established by the Committee of Ministers in agreement with that Party.

Article 23 – Functions of the committee

The Convention Committee:

- a. may make recommendations with a view to facilitating or improving the application of the Convention;

- b. may make proposals for amendment of this Convention in accordance with Article 25;
- c. shall formulate its opinion on any proposal for amendment of this Convention which is referred to it in accordance with Article 25, paragraph 3;
- d. may express an opinion on any question concerning the interpretation or application of this Convention;
- e. shall prepare, before any new accession to the Convention, an opinion for the Committee of Ministers relating to the level of personal data protection of the candidate for accession and, where necessary, recommend measures to take to reach compliance with the provisions of this Convention;
- f. may, at the request of a State or an international organisation, evaluate whether the level of personal data protection the former provides is in compliance with the provisions of this Convention and, where necessary, recommend measures to be taken to reach such compliance;
- g. may develop or approve models of standardised safeguards referred to in Article 14;
- h. shall review the implementation of this Convention by the Parties and recommend measures to be taken in the case where a Party is not in compliance with this Convention;
- i. shall facilitate, where necessary, the friendly settlement of all difficulties related to the application of this Convention.

Article 24 – Procedure

1. The Convention Committee shall be convened by the Secretary General of the Council of Europe. Its first meeting shall be held within twelve months of the entry into force of this Convention. It shall subsequently meet at least once a year, and in any case when one-third of the representatives of the Parties request its convocation.
2. After each of its meetings, the Convention Committee shall submit to the Committee of Ministers of the Council of Europe a report on its work and on the functioning of this Convention.
3. The voting arrangements in the Convention Committee are laid down in the elements for the Rules of Procedure appended to Protocol CETS No. [223].
4. The Convention Committee shall draw up the other elements of its Rules of Procedure and establish, in particular, the procedures for evaluation and review referred to in Article 4, paragraph 3, and Article 23, litterae e, f and h on the basis of objective criteria.

CHAPTER VII – AMENDMENTS

Article 25 – Amendments

1. Amendments to this Convention may be proposed by a Party, the Committee of Ministers of the Council of Europe or the Convention Committee.

2. Any proposal for amendment shall be communicated by the Secretary General of the Council of Europe to the Parties to this Convention, to the other member States of the Council of Europe, to the European Union and to every non-member State or international organisation which has been invited to accede to this Convention in accordance with the provisions of Article 27.

3. Moreover, any amendment proposed by a Party or the Committee of Ministers shall be communicated to the Convention Committee, which shall submit to the Committee of Ministers its opinion on that proposed amendment.

4. The Committee of Ministers shall consider the proposed amendment and any opinion submitted by the Convention Committee and may approve the amendment.

5. The text of any amendment approved by the Committee of Ministers in accordance with paragraph 4 of this article shall be forwarded to the Parties for acceptance.

6. Any amendment approved in accordance with paragraph 4 of this article shall come into force on the thirtieth day after all Parties have informed the Secretary General of their acceptance thereof.

7. Moreover, the Committee of Ministers may, after consulting the Convention Committee, decide unanimously that a particular amendment shall enter into force at the expiration of a period of three years from the date on which it has been opened to acceptance, unless a Party notifies the Secretary General of the Council of Europe of an objection to its entry into force. If such an objection is notified, the amendment shall enter into force on the first day of the month following the date on which the Party to this Convention which has notified the objection has deposited its instrument of acceptance with the Secretary General of the Council of Europe.

CHAPTER VIII – FINAL CLAUSES

Article 26 – Entry into force

1. This Convention shall be open for signature by the member States of the Council of Europe and by the European Union. It is subject to ratification, acceptance or approval. Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.

2. This Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date on which five member States of the Council of Europe have expressed their consent to be bound by the Convention in accordance with the provisions of the preceding paragraph.

3. In respect of any Party which subsequently expresses its consent to be bound by it, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of ratification, acceptance or approval.

Article 27 – Accession by non-member States or international organisations

1. After the entry into force of this Convention, the Committee of Ministers of the Council of Europe may, after consulting the Parties to this Convention and obtaining their unanimous agreement, and in light of the opinion prepared by the Convention Committee in accordance with Article 23.e, invite any State not a member of the Council of Europe or an international organisation to accede to this Convention by a decision taken by the majority provided for in Article 20.d of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the Committee of Ministers.

2. In respect of any State or international organisation acceding to this Convention according to paragraph 1 above, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of accession with the Secretary General of the Council of Europe.

Article 28 – Territorial clause

1. Any State, the European Union or other international organisation may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, specify the territory or territories to which this Convention shall apply.

2. Any State, the European Union or other international organisation may, at any later date, by a declaration addressed to the Secretary General of the Council of Europe, extend the application of this Convention to any other territory specified in the declaration. In respect of such territory the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of receipt of such declaration by the Secretary General.

3. Any declaration made under the two preceding paragraphs may, in respect of any territory specified in such declaration, be withdrawn by a notification addressed to the Secretary General. The withdrawal shall become effective on the first day of the month following the expiration of a period of six months after the date of receipt of such notification by the Secretary General.

Article 29 – Reservations

No reservation may be made in respect of the provisions of this Convention.

Article 30 – Denunciation

1. Any Party may at any time denounce this Convention by means of a notification addressed to the Secretary General of the Council of Europe.

2. Such denunciation shall become effective on the first day of the month following the expiration of a period of six months after the date of receipt of the notification by the Secretary General.

Article 31 – Notifications

The Secretary General of the Council of Europe shall notify the member States of the Council and any Party to this Convention of:

- a. any signature;
- b. the deposit of any instrument of ratification, acceptance, approval or accession;
- c. any date of entry into force of this Convention in accordance with Articles 26, 27 and 28;
- d. any other act, notification or communication relating to this Convention.

APPENDIX TO THE PROTOCOL: ELEMENTS FOR THE RULES OF PROCEDURE OF THE CONVENTION COMMITTEE

1. Each Party has a right to vote and shall have one vote.

2. A two-thirds majority of representatives of the Parties shall constitute a quorum for the meetings of the Convention Committee. In case the amending Protocol to the Convention enters into force in accordance with its Article 37 (2) before its entry into force in respect of all Contracting States to the Convention, the quorum for the meetings of the Convention Committee shall be no less than 34 Parties to the Protocol.

3. The decisions under Article 23 shall be taken by a four-fifths majority. The decisions pursuant to Article 23 litterah shall be taken by a four-fifths majority, including a majority of the votes of States Parties not members of a regional integration organisation that is a Party to the Convention.

4. Where the Convention Committee takes decisions pursuant to Article 23 littera h, the Party concerned by the review shall not vote. Whenever such a decision concerns a matter falling within the competence of a regional integration organisation, neither the organisation nor its member States shall vote.

5. Decisions concerning procedural issues shall be taken by a simple majority.

6. Regional integration organisations, in matters within their competence, may exercise their right to vote in the Convention Committee, with a number of votes equal to the number of their member States that are Parties to the Convention. Such an organisation shall not exercise its right to vote if any of its member States exercises its right.

7. In case of vote, all Parties must be informed of the subject and time for the vote, as well as whether the vote will be exercised by the Parties individually or by a regional integration organisation on behalf of its member States.

8. The Convention Committee may further amend its rules of procedure by a two-thirds majority, except for the voting arrangements which may only be amended by unanimous vote of the Parties and to which Article 25 of the Convention applies.

Convention on Cybercrime[1]
(Budapest Convention)

Budapest, 23/11/2001 **– Treaty (ETS No.185) open for signature by the member States of the Council of Europe and the non-member States which have participated in its elaboration and for accession by other non-member States**

PREAMBLE

The member States of the Council of Europe and the other States signatory hereto,

Considering that the aim of the Council of Europe is to achieve a greater unity between its members;

Recognising the value of fostering co-operation with the other States parties to this Convention;

Convinced of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, inter alia, by adopting appropriate legislation and fostering international co-operation;

Conscious of the profound changes brought about by the digitalisation, convergence and continuing globalisation of computer networks;

Concerned by the risk that computer networks and electronic information may also be used for committing criminal offences and that evidence relating to such offences may be stored and transferred by these networks;

Recognising the need for co-operation between States and private industry in combating cybercrime and the need to protect legitimate interests in the use and development of information technologies;

Believing that an effective fight against cybercrime requires increased, rapid and well-functioning international co-operation in criminal matters;

1. Source : Treaty Office on conventions.coe.int

Convinced that the present Convention is necessary to deter action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data by providing for the criminalisation of such conduct, as described in this Convention, and the adoption of powers sufficient for effectively combating such criminal offences, by facilitating their detection, investigation and prosecution at both the domestic and international levels and by providing arrangements for fast and reliable international co-operation;

Mindful of the need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights as enshrined in the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights and other applicable international human rights treaties, which reaffirm the right of everyone to hold opinions without interference, as well as the right to freedom of expression, including the freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, and the rights concerning the respect for privacy;

Mindful also of the right to the protection of personal data, as conferred, for example, by the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data;

Considering the 1989 United Nations Convention on the Rights of the Child and the 1999 International Labour Organization Worst Forms of Child Labour Convention;

Taking into account the existing Council of Europe conventions on co-operation in the penal field, as well as similar treaties which exist between Council of Europe member States and other States, and stressing that the present Convention is intended to supplement those conventions in order to make criminal investigations and proceedings concerning criminal offences related to computer systems and data more effective and to enable the collection of evidence in electronic form of a criminal offence;

Welcoming recent developments which further advance international understanding and co-operation in combating cybercrime, including action taken by the United Nations, the OECD, the European Union and the G8;

Recalling Committee of Ministers Recommendations No. R (85) 10 concerning the practical application of the European Convention on Mutual Assistance in Criminal Matters in respect of letters rogatory for the interception of telecommunications, No. R (88) 2 on piracy in the field of copyright and neighbouring rights, No. R (87) 15 regulating the use of personal data in the police sector, No. R (95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services, as well as No. R (89) 9 on computer-related crime providing guidelines for national legislatures concerning the definition of certain computer crimes and No. R (95) 13 concerning problems of criminal procedural law connected with information technology;

Having regard to Resolution No. 1 adopted by the European Ministers of Justice at their 21st Conference (Prague, 10 and 11 June 1997), which recommended that the Committee of Ministers support the work on cybercrime carried out by the European Committee on Crime Problems (CDPC) in order to bring domestic criminal law provisions closer to each other and enable the use of effective means of investigation into such offences, as well as to Resolution No. 3 adopted at the 23rd Conference of the European Ministers of Justice (London, 8 and 9 June 2000), which encouraged the negotiating parties to pursue their efforts with a view to finding appropriate solutions to enable the largest possible number of States to become parties to the Convention and acknowledged the need for a swift and efficient system of international co-operation, which duly takes into account the specific requirements of the fight against cybercrime;

Having also regard to the Action Plan adopted by the Heads of State and Government of the Council of Europe on the occasion of their Second Summit (Strasbourg, 10 and 11 October 1997), to seek common responses to the development of the new information technologies based on the standards and values of the Council of Europe;

Have agreed as follows:

CHAPTER I – USE OF TERMS

Article 1 – Definitions

For the purposes of this Convention:

- a. "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;

- b. "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;

- c. "service provider" means:

  i. any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and

  ii. any other entity that processes or stores computer data on behalf of such communication service or users of such service.

- d. "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.

CHAPTER II – MEASURES TO BE TAKEN AT THE NATIONAL LEVEL
Section 1 – Substantive criminal law

Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems

Article 2 – Illegal access

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 3 – Illegal interception

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 4 – Data interference

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.

2. A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

Article 5 – System interference

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

Article 6 – Misuse of devices

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:

   - a. the production, sale, procurement for use, import, distribution or otherwise making available of:

     i. a device, including a computer program, designed or adapted primarily

for the purpose of committing any of the offences established in accordance with Articles 2 through 5;

ii. a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and

- b. the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

2. This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.

3. Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.

Title 2 – Computer-related offences

Article 7 – Computer-related forgery

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

Article 8 – Computer-related fraud

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:

- a. any input, alteration, deletion or suppression of computer data,

- b. any interference with the functioning of a computer system,

with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

Title 3 – Content-related offences

Article 9 – Offences related to child pornography

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:
   - a. producing child pornography for the purpose of its distribution through a computer system;
   - b. offering or making available child pornography through a computer system;
   - c. distributing or transmitting child pornography through a computer system;
   - d. procuring child pornography through a computer system for oneself or for another person;
   - e. possessing child pornography in a computer system or on a computer-data storage medium.
2. For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts:
   - a. a minor engaged in sexually explicit conduct;
   - b. a person appearing to be a minor engaged in sexually explicit conduct;
   - c. realistic images representing a minor engaged in sexually explicit conduct.
3. For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.
4. Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d and e, and 2, sub-paragraphs b and c.

Title 4 – Offences related to infringements of copyright and related rights

Article 10 – Offences related to infringements of copyright and related rights

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.
2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection

of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

3. A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.

Title 5 – Ancillary liability and sanctions

Article 11 – Attempt and aiding or abetting

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed.

2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c of this Convention.

3. Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.

Article 12 – Corporate liability

1. Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on:

   - a. a power of representation of the legal person;

   - b. an authority to take decisions on behalf of the legal person;

   - c. an authority to exercise control within the legal person.

2. In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal

offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority.

3. Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative.

4. Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.

Article 13 – Sanctions and measures

1. Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty.

2. Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.

Section 2 – procedural law

Title 1 – Common provisions

Article 14 – Scope of procedural provisions

1. Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings.

2. Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:

   - a. the criminal offences established in accordance with Articles 2 through 11 of this Convention;
   - b. other criminal offences committed by means of a computer system; and
   - c. the collection of evidence in electronic form of a criminal offence.

3. - a. Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20.
   - b. Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system:

     i. is being operated for the benefit of a closed group of users, and

ii. does not employ public communications networks and is not connected with another computer system, whether public or private,

that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21.

Article 15 – Conditions and safeguards

1. Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.

2. Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, inter alia, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.

3. To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.

Title 2 – Expedited preservation of stored computer data

Article 16 – Expedited preservation of stored computer data

1. Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.

2. Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.

3. Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.

4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Article 17 – Expedited preservation and partial disclosure of traffic data

1. Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to:

   - a. ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and

   - b. ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted.

2. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Title 3 – Production order

Article 18 – Production order

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:

   - a. a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and

   - b. a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.

2. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

3. For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:

   - a. the type of communication service used, the technical provisions taken thereto and the period of service;

   - b. the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;

- c. any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

Title 4 – Search and seizure of stored computer data

Article 19 – Search and seizure of stored computer data

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:

   - a. a computer system or part of it and computer data stored therein; and

   - b. a computer-data storage medium in which computer data may be stored in its territory.

2. Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.

3. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:

   - a. seize or similarly secure a computer system or part of it or a computer-data storage medium;

   - b. make and retain a copy of those computer data;

   - c. maintain the integrity of the relevant stored computer data;

   - d. render inaccessible or remove those computer data in the accessed computer system.

4. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.

5. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Title 5 – Real-time collection of computer data

Article 20 – Real-time collection of traffic data

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:

   - a. collect or record through the application of technical means on the territory of that Party, and

   - b. compel a service provider, within its existing technical capability:

     I. to collect or record through the application of technical means on the territory of that Party; or

     ii. to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.

2. Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory.

3. Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Article 21 – Interception of content data

1. Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to:

   - a. collect or record through the application of technical means on the territory of that Party, and

   - b. compel a service provider, within its existing technical capability:

     i. to collect or record through the application of technical means on the territory of that Party, or

     ii. to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system.

2. Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt

legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory.

3. Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Section 3 – Jurisdiction

Article 22 – Jurisdiction

1. Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:

   - a. in its territory; or
   - b. on board a ship flying the flag of that Party; or
   - c. on board an aircraft registered under the laws of that Party; or
   - d. by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.

2. Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof.

3. Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.

4. This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.

5. When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.

CHAPTER III – INTERNATIONAL CO-OPERATION
Section 1 – General principles

Title 1 – General principles relating to international co-operation
Article 23 – General principles relating to international co-operation

The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through the application of relevant international instruments on international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

Title 2 – Principles relating to extradition
Article 24 – Extradition

1. ▸ a. This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty.

   ▸ b. Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply.

2. The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them.

3. If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article.

4. Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves.

5. Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition.

6. If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because

the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party.

7. ▸ a. Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty.

   ▸ b. The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

Title 3 – General principles relating to mutual assis tance

Article 25 – General principles relating to mutual assistance

1. The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

2. Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35.

3. Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication.

4. Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence.

5. Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether

its place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.

Article 26 – Spontaneous information

1. A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter.

2. Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.

Title 4 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

1. Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.

2. ▸ a. Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution.

   ▸ b. The central authorities shall communicate directly with each other;

   ▸ c. Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph;

   ▸ d. The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

3. Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party.

4. The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if:

   - a. the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or

   - b. it considers that execution of the request is likely to prejudice its sovereignty, security, ordre public or other essential interests.

5. The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities.

6. Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary.

7. The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly.

8. The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

9. - a. In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party.

   - b. Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol).

   - c. Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so.

- d. Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party.
- e. Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.

Article 28 – Confidentiality and limitation on use

1. When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.

2. The requested Party may make the supply of information or material in response to a request dependent on the condition that it is:
   - a. kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or
   - b. not used for investigations or proceedings other than those stated in the request.

3. If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it.

4. Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.

Section 2 – Specific provisions

Title 1 – Mutual assistance regarding provisional measures

Article 29 – Expedited preservation of stored computer data

1. A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data.

2. A request for preservation made under paragraph 1 shall specify:
   - a. the authority seeking the preservation;

- b. the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;

- c. the stored computer data to be preserved and its relationship to the offence;

- d. any available information identifying the custodian of the stored computer data or the location of the computer system;

- e. the necessity of the preservation; and

- f. that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data.

3. Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation.

4. A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled.

5. In addition, a request for preservation may only be refused if:

   - a. the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or

   - b. the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, ordre public or other essential interests.

6. Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

7. Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty days, in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request.

Article 30 – Expedited disclosure of preserved traffic data

1. Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted.

2. Disclosure of traffic data under paragraph 1 may only be withheld if:

   - a. the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or
   - b. the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, ordre public or other essential interests.

Title 2 – Mutual assistance regarding investigative powers

Article 31 – Mutual assistance regarding accessing of stored computer data

1. A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29.

2. The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter.

3. The request shall be responded to on an expedited basis where:

   - a. there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or
   - b. the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.

Article 32 – Trans-border access to stored computer data with consent or where publicly available

A Party may, without the authorisation of another Party:

   - a. access publicly available (open source) stored computer data, regardless of where the data is located geographically; or
   - b. access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

Article 33 – Mutual assistance regarding the real-time collection of traffic data

1. The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law.

2. Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.

Article 34 – Mutual assistance regarding the interception of content data

The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.

Title 3 – 24/7 Network

Article 35 – 24/7 Network

1. Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures:

   - a. the provision of technical advice;

   - b. the preservation of data pursuant to Articles 29 and 30;

   - c. the collection of evidence, the provision of legal information, and locating of suspects.

2. - a. A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis.

   - b. If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis.

3. Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.

CHAPTER IV – FINAL PROVISIONS

Article 36 – Signature and entry into force

1. This Convention shall be open for signature by the member States of the Council of Europe and by non-member States which have participated in its elaboration.

2. This Convention is subject to ratification, acceptance or approval. Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.

3. This Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date on which five States, including at least three member States of the Council of Europe, have expressed their consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.

4. In respect of any signatory State which subsequently expresses its consent to be bound by it, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of the expression of its consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.

Article 37 – Accession to the Convention

1. After the entry into force of this Convention, the Committee of Ministers of the Council of Europe, after consulting with and obtaining the unanimous consent of the Contracting States to the Convention, may invite any State which is not a member of the Council and which has not participated in its elaboration to accede to this Convention. The decision shall be taken by the majority provided for in Article 20.d. of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the Committee of Ministers.

2. In respect of any State acceding to the Convention under paragraph 1 above, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of accession with the Secretary General of the Council of Europe.

Article 38 – Territorial application

1. Any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, specify the territory or territories to which this Convention shall apply.

2. Any State may, at any later date, by a declaration addressed to the Secretary General of the Council of Europe, extend the application of this Convention to any other territory specified in the declaration. In respect of such territory the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of receipt of the declaration by the Secretary General.

3. Any declaration made under the two preceding paragraphs may, in respect of any territory specified in such declaration, be withdrawn by a notification addressed to the Secretary General of the Council of Europe. The withdrawal shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of such notification by the Secretary General.

Article 39 – Effects of the Convention

1. The purpose of the present Convention is to supplement applicable multilateral or bilateral treaties or arrangements as between the Parties, including the provisions of:

   - the European Convention on Extradition, opened for signature in Paris, on 13 December 1957 (ETS No. 24);
   - the European Convention on Mutual Assistance in Criminal Matters, opened for signature in Strasbourg, on 20 April 1959 (ETS No. 30);
   - the Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, opened for signature in Strasbourg, on 17 March 1978 (ETS No. 99).

2. If two or more Parties have already concluded an agreement or treaty on the matters dealt with in this Convention or have otherwise established their relations on such matters, or should they in future do so, they shall also be entitled to apply that agreement or treaty or to regulate those relations accordingly. However, where Parties establish their relations in respect of the matters dealt with in the present Convention other than as regulated therein, they shall do so in a manner that is not inconsistent with the Convention's objectives and principles.

3. Nothing in this Convention shall affect other rights, restrictions, obligations and responsibilities of a Party.

Article 40 – Declarations

By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the possibility of requiring additional elements as provided for under Articles 2, 3, 6 paragraph 1.b, 7, 9 paragraph 3, and 27, paragraph 9.e.

Article 41 – Federal clause

1. A federal State may reserve the right to assume obligations under Chapter II of this Convention consistent with its fundamental principles governing the relationship between its central government and constituent States or other similar territorial entities provided that it is still able to co-operate under Chapter III.

2. When making a reservation under paragraph 1, a federal State may not apply the terms of such reservation to exclude or substantially diminish its obligations to provide for measures set forth in Chapter II. Overall, it shall provide for a broad and effective law enforcement capability with respect to those measures.

3. With regard to the provisions of this Convention, the application of which comes under the jurisdiction of constituent States or other similar territorial entities, that are not obliged by the constitutional system of the federation to take legislative measures, the federal government shall inform the competent authorities of such States of the said provisions with its favourable opinion, encouraging them to take appropriate action to give them effect.

Article 42 – Reservations

By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.

Article 43 – Status and withdrawal of reservations

1. A Party that has made a reservation in accordance with Article 42 may wholly or partially withdraw it by means of a notification addressed to the Secretary General of the Council of Europe. Such withdrawal shall take effect on the date of receipt of such notification by the Secretary General. If the notification states that the withdrawal of a reservation is to take effect on a date specified therein, and such date is later than the date on which the notification is received by the Secretary General, the withdrawal shall take effect on such a later date.

2. A Party that has made a reservation as referred to in Article 42 shall withdraw such reservation, in whole or in part, as soon as circumstances so permit.

3. The Secretary General of the Council of Europe may periodically enquire with Parties that have made one or more reservations as referred to in Article 42 as to the prospects for withdrawing such reservation(s).

Article 44 – Amendments

1. Amendments to this Convention may be proposed by any Party, and shall be communicated by the Secretary General of the Council of Europe to the member States of the Council of Europe, to the non-member States which have participated in the elaboration of this Convention as well as to any State which has acceded to, or has been invited to accede to, this Convention in accordance with the provisions of Article 37.

2. Any amendment proposed by a Party shall be communicated to the European Committee on Crime Problems (CDPC), which shall submit to the Committee of Ministers its opinion on that proposed amendment.

3. The Committee of Ministers shall consider the proposed amendment and the opinion submitted by the CDPC and, following consultation with the non-member States Parties to this Convention, may adopt the amendment.

4. The text of any amendment adopted by the Committee of Ministers in accordance with paragraph 3 of this article shall be forwarded to the Parties for acceptance.

5. Any amendment adopted in accordance with paragraph 3 of this article shall come into force on the thirtieth day after all Parties have informed the Secretary General of their acceptance thereof.

Article 45 – Settlement of disputes

1. The European Committee on Crime Problems (CDPC) shall be kept informed regarding the interpretation and application of this Convention.

2. In case of a dispute between Parties as to the interpretation or application of this Convention, they shall seek a settlement of the dispute through negotiation or any other peaceful means of their choice, including submission of the dispute to the CDPC, to an arbitral tribunal whose decisions shall be binding upon the Parties, or to the International Court of Justice, as agreed upon by the Parties concerned.

Article 46 – Consultations of the Parties

1. The Parties shall, as appropriate, consult periodically with a view to facilitating:

   - a. the effective use and implementation of this Convention, including the identification of any problems thereof, as well as the effects of any declaration or reservation made under this Convention;

   - b. the exchange of information on significant legal, policy or technological developments pertaining to cybercrime and the collection of evidence in electronic form;

   - c. consideration of possible supplementation or amendment of the Convention.

2. The European Committee on Crime Problems (CDPC) shall be kept periodically informed regarding the result of consultations referred to in paragraph 1.

3. The CDPC shall, as appropriate, facilitate the consultations referred to in paragraph 1 and take the measures necessary to assist the Parties in their efforts to supplement or amend the Convention. At the latest three years after the present Convention enters into force, the European Committee on Crime Problems (CDPC) shall, in co-operation with the Parties, conduct a review of

all of the Convention's provisions and, if necessary, recommend any appropriate amendments.

4. Except where assumed by the Council of Europe, expenses incurred in carrying out the provisions of paragraph 1 shall be borne by the Parties in the manner to be determined by them.

5. The Parties shall be assisted by the Secretariat of the Council of Europe in carrying out their functions pursuant to this article.

Article 47 – Denunciation

1. Any Party may, at any time, denounce this Convention by means of a notification addressed to the Secretary General of the Council of Europe.

2. Such denunciation shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of the notification by the Secretary General.

Article 48 – Notification

The Secretary General of the Council of Europe shall notify the member States of the Council of Europe, the non-member States which have participated in the elaboration of this Convention as well as any State which has acceded to, or has been invited to accede to, this Convention of:

- a. any signature;
- b. the deposit of any instrument of ratification, acceptance, approval or accession;
- c. any date of entry into force of this Convention in accordance with Articles 36 and 37;
- d. any declaration made under Article 40 or reservation made in accordance with Article 42;
- e. any other act, notification or communication relating to this Convention.

In witness whereof the undersigned, being duly authorised thereto, have signed this Convention.

Done at Budapest, this 23rd day of November 2001, in English and in French, both texts being equally authentic, in a single copy which shall be deposited in the archives of the Council of Europe. The Secretary General of the Council of Europe shall transmit certified copies to each member State of the Council of Europe, to the non-member States which have participated in the elaboration of this Convention, and to any State invited to accede to it.

T-CY Guidance Note No. 9[1]

Aspects of election interference by means of computer systems covered by the Budapest Convention

Adopted by Cybercrime Convention Committee (T-CY) 21 on 8 July 2019

1. INTRODUCTION

The Cybercrime Convention Committee (T-CY) at its 8th Plenary (December 2012) decided to issue Guidance Notes aimed at facilitating the effective use and implementation of the Budapest Convention on Cybercrime, also in the light of legal, policy and technological developments.[2]

Guidance Notes represent the common understanding of the Parties to this treaty regarding the use of the Convention.

Interference with elections through malicious cyber activities against computers and data used in elections and election campaigns undermines free, fair and clean elections and trust in democracy. Disinformation operations, as experienced in particular since 2016, may make use of malicious cyber activities and may have the same effect. Domestic election procedures may need to be adapted to the realities of the information society, and computer systems used in elections and related campaigns need to be made more secure.

In this context, greater efforts need to be undertaken to prosecute such interference where it constitutes a criminal offence: an effective criminal justice response may deter election interference and reassure the electorate with regard to the use of information and communication technologies in elections.

The present Note addresses how Articles of the Convention may apply to aspects of election interference by means of computer systems.

The substantive criminal offences of the Convention may be carried out as acts of election interference or as preparatory acts facilitating such interference.

1. Source: www.coe.int/TCY
2. See the mandate of the T-CY (Article 46 Budapest Convention).

In addition, the domestic procedural and international mutual legal assistance tools of the Convention are available for investigations and prosecutions related to election interference. The scope and limits of procedural powers and tools for international cooperation are defined by Articles 14.2 and 25.1 Budapest Convention:

Article 14.2

Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:

- a. the criminal offences established in accordance with Articles 2 through 11 of this Convention;
- b. other criminal offences committed by means of a computer system; and
- c. the collection of evidence in electronic form of a criminal offence.

Article 25.1

The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

The procedural powers of the Convention are subject to the conditions and safeguards of Article.

2. RELEVANT PROVISIONS OF THE BUDAPEST CONVENTION ON CYBERCRIME (ETS 185)

2.1 Procedural provisions

The Convention's procedural powers (Articles 14-21) may be used in a specific criminal investigation or proceeding in any type of election interference, as Article 14 provides.

The specific procedural measures can be very useful in criminal investigations of election interference. For example, in cases of election interference, a computer system may be used to commit or facilitate an offence, the evidence of that offence may be stored in electronic form, or a suspect may be identifiable through subscriber information, including an Internet Protocol address. Similarly, illegal political financing may be traceable via preserved email, voice communications between conspirators may be captured pursuant to properly authorised interception, and misuse of data may be illustrated by electronic trails.

Thus, in criminal investigations of election interference, Parties may use expedited preservation of stored computer data, production orders, search and seizure of stored computer data, and other tools to collect electronic evidence needed for the investigation and prosecution of such offences relating to election interference.

2.2 International mutual legal assistance provisions

The Convention's international cooperation powers (Articles 23-35) are of similar breadth and may assist Parties in investigations of election interference.

Thus, Parties shall make available expedited preservation of stored computer data, production orders, search and seizure of stored computer data, as well as other international cooperation provisions.

2.3 Substantive criminal law provisions

Finally, as noted above, election interference may involve the following types of conduct, when done without right, as criminalised by the Convention on Cybercrime. The T-CY emphasises that the examples below are merely examples – that is, since election interference is a developing phenomenon, it may appear in many forms not listed below. However, the T-CY expects that the Convention on Cybercrime is sufficiently flexible to address them.

Relevant Articles	Examples
Article 2 – Illegal access	A computer system may be illegally accessed to obtain sensitive or confidential information related to candidates, campaigns, political parties or voters.
Article 3 – Illegal interception	Non-public transmissions of computer data to, from, or within a computer system may be illegally intercepted to obtain sensitive or confidential information related to candidates, campaigns, political parties or voters.
Article 4 – Data interference	Computer data may be damaged, deleted, deteriorated, altered, or suppressed to modify websites, to alter voter databases, or to manipulate results of votes such as by tampering with voting machines.
Article 5 – System interference	The functioning of computer systems used in elections or campaigns may be hindered to interfere with campaign messaging, hinder voter registration, disable the casting of votes or prevent the counting of votes through denial of service attacks, malware or other means.
Article 6 – Misuse of devices	The sale, procurement for use, import, distribution or other acts making available computer passwords, access codes, or similar data by which computer systems may be accessed may facilitate election interference such as the theft of sensitive data from political candidates, parties or campaigns.

Relevant Articles	Examples
Article 7 – Computer-related forgery	Computer data (for example the data used in voter databases) may be input, altered, deleted, or suppressed with the result that inauthentic data is considered or acted upon for legal purposes as if it were authentic. For example, some countries require election campaigns to make public financial disclosures. Forgery of computer data could create the impression of incorrect disclosures or hide questionable sources of campaign funds.
Article 11 – Attempt, aiding and abetting	Crimes specified in the treaty may be attempted, aided or abetted in furtherance of election interference.
Article 12 – Corporate liability	Crimes covered by Articles 2-11 of the Convention in furtherance of election interference may be carried out by legal persons that would be liable under Article 12.
Article 13 – Sanctions	Crimes covered by the Convention may pose a threat to individuals and to society, especially when the crimes are directed against fundamentals of political life such as elections. Criminal actions and their effects may differ in different countries, but election interference may undermine trust in democratic processes, change the outcome of an election, require the expense and upheaval of a second election, or cause physical violence between election partisans and communities. A Party may provide in its domestic law a sanction that is unsuitably lenient for election-related acts in relation to Articles 2 - 11, and it may not permit the consideration of aggravated circumstances or of attempt, aiding or abetting. This may mean that Parties need to consider amendments to their domestic law. Parties should ensure, pursuant to Article 13 that criminal offences related to such acts "are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty". Parties may also consider aggravating circumstances, for example, if such acts affect an election significantly or cause deaths or physical injuries or significant material damage.

3. T-CY STATEMENT

The T-CY agrees that the substantive offences in the Convention may also be acts of election interference as defined in applicable law, that is, offences against free, fair and clean elections.

The substantive crimes in the Convention may be carried out to facilitate, participate in or prepare acts of election interference.

The procedural and mutual legal assistance tools in the Convention may be used to investigate election interference, its facilitation, participation in it, or preparatory acts.

CDL-AD(2019)016

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 (DGI) on Digital Technologies and Elections[1]

Adopted by the Council of Democratic Elections
At its 65th meeting (Venice, 20 June 2019)

Adopted by the Venice Commission at its 119th Plenary Session
(Venice, 21 – 22 June 2019)

On the basis of comments by
Mr Richard BARRETT (Member, Ireland)
Ms Herdis KJERULF THORGEIRSDOTTIR (Member, Iceland)
Mr Rafael RUBIO NUÑEZ (Substitute Member, Spain)
Mr José Luis VARGAS VALDEZ (Substitute Member, Mexico)
Ms Krisztina ROZGONYI (DGI Expert, Media and Internet Governance Division)
Ms Nevena RUZIC (DGI Expert, Data Protection Division)

I. INTRODUCTION

1. At its 59th meeting (15 June 2017), the Council for Democratic Elections, upon an initiative by Mr José Luis Vargas Valdez and on the basis of his "Study on the role of social media and the internet in democratic development" (CDL-LA(2018)001), decided to undertake a study on the use of digital technologies during electoral processes, jointly with the Council of Europe's Information Society Department.

2. In addition to Mr Vargas Valdez, Ms Herdis Kjerulf Thorgeirsdóttir, Mr Richard Barrett and Mr Rafael Rubio Nuñez acted as rapporteurs. Ms Krisztina Rozgonyi and Ms Nevena Ružić acted as experts on behalf of the Information Society and Action against Crime Directorate, Media and Internet Governance Division and of the Data Protection Division respectively. Mr Alexander Seger, head of the Cybercrime Division, also contributed to the relevant parts of this joint report.

3. This joint report was prepared on the basis of Mr Vargas Valdez's original study and of the comments submitted by the rapporteurs and experts above; it was examined at the meeting of the Sub-Commission on Latin America on

1. Source: venice.coe.int

30 November 2018, adopted by the Council for Democratic Elections at its 65th meeting (Venice, 20 June 2019) and subsequently adopted by the Venice Commission at its 119th plenary session (Venice, 21-22 June 2019).

II. BACKGROUND

4. Digital (or "new") technologies and social media – the latter being understood as "internet platforms that allow for bidirectional interaction through users-generated content"[2] – have revolutionised the way people interact and exercise their freedom of expression and information, as well as other related - and sometimes conflicting – fundamental rights.[3] People who engage in social media may use the internet to organise and demand better services, more transparency and meaningful participation in the political arena.[4] Individuals all over the globe are now able to shape global perceptions, position topics in their national agendas and foster political activism.[5] This digital transformation is recasting the relation between states and citizens.

5. According to the Global Digital Report 2018, more than half of the world's web traffic now comes from mobile phones. From a total of 7.6 billion inhabitants of the world, roughly 4 billion are internet users (which represents 53% of the total population), and 3.2 billion are social media active users (which represents 42% of the total population).

6. Between 2017 and 2018, the number of internet users increased by 7% and active social media users increased by 13%. The average internet user spends around 6 hours online each day. Much of this time will be spent in social media platforms like Facebook (with 2,167 million users), Youtube (1,500 millions), Instagram (800 millions) or Twitter (330 millions).

7. Today approximately two billion internet users are using social networks[6] on a daily basis, and social media have become an indispensable part of modern political campaigning, their effects on the public being dependent on multiple

2. This study adopts a definition of social media as "web or mobile-based platforms that allow for two-way interactions through user-generated content (UGC) and communication. Social media are therefore not media that originate only from one source or are broadcast from a static website. Rather, they are media on specific platforms designed to allow users to create ("generate") content and to interact with the information and its source (International IDEA 2014: 11). While social media rely on the internet as a medium, it is important to note that not all internet sites or platforms meet the definition of social media. Some websites make no provision for interactivity with the audience, while others allow users only to post comments as a reaction to particular published content as discussions posts (or "threads") which are moderated and controlled" (International IDEA 2014: 11).
3. Parliamentary Assembly of the Council of Europe, Resolution 1987 [2014] on the right to internet access.
4. Santiso, 2018.
5. There are notable examples of this: from the Egyptian teenagers who used Facebook to rally protesters to Tahrir Square, to the influence of disinformation on the outcome of the Kenyan Presidential Election, to the Chileans who campaigned online to make overseas voting a key election issue with "Haz tu voto volar" or the fact-checking project "Verificado 2018" in Mexico.
6. Statista – Most popular social networks worldwide as of October 2018. Available at: www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users Dimitrova & Matthes, 2018

factors such as channel-variables (e.g. Twitter vs. Instagram), specific audience characteristics and predispositions, user motivations and the political campaign context overall.[7]

8. Even though everyone seems to use the internet and social media, different age groups use them for different purposes. According to the ***Reuters Institute Digital News Report 2017***, social media tends to be the main source of news for people between 18 and 34 years old, whereas television is more important for people above 55.

9. According to the same study of the Reuters Institute, more than half of the respondents (54%) prefer paths that use algorithms to select stories (search engines, social media, and many aggregators) rather than editors or journalists (44%). This means that young citizens might be making political decisions based on the information filtered by the algorithms of such digital environments, instead of on strict journalistic standards. At the same time, it should be noted that according to recent research,[8] personalised recommendations through algorithmic selection may provide just as diverse news offers as human editorial selection.

10. According to the ***Reuters Institute Digital News Report 2018,*** the use of social media for accessing news decreased in 2017. People seemed to have less trust in the social media sources. It has also been observed that "[t]he internet has quickly moved from primarily being used for information access to become a participatory environment more closely mimicking the democratic participation traditional in the physical world".[9] As a consequence, the massive use of the internet and social media platforms around the world is changing many aspects of our social and political life. The social mechanisms of knowledge and opinion making are becoming more collaborative and self-regulated (e.g. Wikipedia, Facebook) and political activism has found new and efficient ways of organisation and expression.[10]

11. In its beginnings, the internet was hailed as a promise of equality and liberty. It was seen as a potential ***new public sphere***, the platform of democratic public discourse, empowering individuals to be active participants in the public discourse and hence contributing to a more efficient political democracy with an enlightened public due to the active discourse on social media. The public sphere used to be hierarchically organised with set and established functions of various players such as the State, the media, the church or educational institutions, all of which have today lost control over the horizon-

7. Dimitrova & Matthes, 2018.
8. See www.tandfonline.com/doi/abs/10.1080/1369118X.2018.1444076 and www.thatseemsimportant.com/content/blame-the-algorithm
9. Laidlaw 2015, p. 7.
10. Castells 2011; Cohen et al. 2012.

tal interchange of news and views among the users. The social media promised to give everyone a voice. In contrast with the traditional mass media, the internet has an open-ended multidirectional architecture, and the access costs are relatively low. These traits make the internet a particularly effective media for common citizens to become active speakers instead of just receivers of information and have created a "networked public sphere", where individuals can "monitor and disrupt the use of mass media power" thanks to the immediate access to several sources of information and data distribution.

12. In the past, journalists with their editorial practices and ethical obligations held the gatekeeper role in communication, not only deciding what was fit to print or publish, but also in charge of adherence to the statutory requirements, such as a fair and balanced coverage with regard to the public service media, respecting silence periods where relevant, and/or the right of reply and equivalent remedies for candidates and political parties. Now this gatekeeping function is increasingly taken over by new intermediaries. Such companies include internet service providers (ISPs), search engines and social media platforms.[11] The ***Internet intermediaries*** are organizations (primarily, for-profit companies) that "bring together or facilitate transactions between third parties on the Internet. They give access to, host, transmit and index content, products and services originated by third parties on the Internet or provide Internet-based services to third parties". These have hence acquired control over the flow, availability, findability and accessibility of information and other content online.[12]

13. The internet's great promise was that it operated outside the purview of existing communications monopolies but in reality large multinational corporations[13] have global control over the flow of information and are thus in a position to shape the political discourse and opinion formation. The same forces are at work as in the traditional media landscape but now their voices are amplified by social media and they are able to reach every corner of the world and transform societies and lives. The notion that the internet should afford at least a minimally competitive landscape for new entrants seems no longer relevant. The few private actors who own the information superhighways are powerful and deregulated enough to dictate conditions on social, individual and political freedoms, thus becoming a third actor in the democratic arena; and content production has become so "democratic" and anonymous that it is

11. The term "internet intermediaries" refers to the operators of online media platforms, of search engines, social networks and app stores (van der Noll, Helberger, & Kleinen-von Königslöw, 2015). According to the Council of Europe's Recommendation CM/Rec(2018)2 on the roles and responsibilities of internet intermediaries, these players facilitate interactions on the internet between natural and legal persons by offering and performing a variety of functions and services. Some connect users to the internet, enable the processing of information and data, or host web-based services, including for user-generated content. Others aggregate information and enable searches; they give access to, host and index content and services designed and/or operated by third parties. Some facilitate the sale of goods and services, including audio-visual services, and enable other commercial transactions, including payments.

12. www-cdn.law.stanford.edu/wp-content/uploads/2017/04/07_28.2_Persily-web.pdf

13. See e.g. www.forbes.com/sites/steveandriole/2018/09/26/apple-google-microsoft-amazon-and-facebookown-huge-market-shares-technology-oligarchy/#372d73d92318.

extremely difficult to identify trustworthy information and attribute responsibilities for illegal behaviours online.

14. The social media, like Facebook, is no less than the traditional media controlled by market forces. The stock price of Facebook like any big media corporations depends on its advertisement revenues; to grow financially and sustain its market value. Advertising on Facebook works by determining its users' interests, based on data it collects from their browsing, likes and so on, through a very hi-tech operation. The sites make money from clicks, and through algorithmic regulation create echo chambers and filter bubbles where individuals receive the kinds of information that they have either preselected, or, more ominously, that algorithms have figured out they want to hear. This allows for political advertising to be increasingly individually tailored and targeted. Instead of being a public square featuring many voices people are becoming more isolated and out of touch with the whole spectrum of the public.

15. The "democratisation" of content production and the centralisation of online distribution channels have had as unintended consequence the proliferation of false information, private and public disinformation tactics. The advent of every means of communication (1) expands the dissemination of and the access to information (freedom of communication); (2) implies the risk of abuses (malicious content); (3) opens the way to censorship and (4) to manipulation by the powerful public and private actors.

16. The development of internet and of social media has brought mass communication and the imparting and receiving process to a scale of dimensions unkown since the creation of the printing press. The proliferation of false information, private and public disinformation tactics has therefore become significantly more widespread and technically sophisticated over the last few years, with bots, propaganda producers, disinformation outlets exploiting social media and search algorithms that ensure high visibility and seamless integration with trusted content, misleading large audiences of news consumers, and more importantly, voters. While disinformation has always been a strategy to discredit opponents and to sway political support to one side or the other, digital technologies have increased the threats of false information to democracy for different reasons: the speed of dissemination of (false) information through the internet;[14] the fact that they are actually facilitated by the current architecture of search-engines and social media; the lack of tools (either legal, social or technical) to identify them and stop their spread; and the difficulty of investigating and prosecuting such online behaviour.

14. Evidence is also now available that people are more likely to share untrue news. Moreover, according to the largest ever-made study of this phenomenon in digital media done by the MIT, false information is more prone to circulate through digital means. It would furthermore appear that it takes true stories about six times as long as false stories to reach people (Vosoughi, Roy and Aral, 2018). According to the Edelman Trust Barometer 2018 Global Report nearly 70% of the global internet users worry about "fake news" being used as a weapon.

17. In recent years, foreign intervention in elections through the use of social media has also become a concern for democracies. Technological resources such as low-cost digital espionage campaigns, paid users and bots, selective disclosure of information or creation of false information has changed the rules of the game during electoral campaigns. As a side effect, this has eroded confidence in democratic governments.

18. At a global scale, the above-mentioned practices – which are facilitated by digital technologies – may pose a threat to democracy and question the idea of the internet as a technological means for more democratic governance.

19. 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. This study is not intended at assessing its positive and negative aspects, but at meeting the challenges it presents in the electoral field. It will therefore mainly focus more on the problems the innovation raises and on their possible solutions than on its advantages.

20. The present report does not intend to provide concrete and universal solutions for all problems that the use of the internet and social media might entail in all electoral processes. The particularities of each nation and each democracy would make it an impossible task.[15] Instead, its purpose is to identify the most relevant legal problems caused by the use of those technologies, describe their logic and possible solution parameters, point out the shortcomings identified so far, and suggest a general set of principles and guidelines that might help to adapt democracy and its laws to the new technological realities. In this sense, the conclusion of this work resembles a roadmap to existing and future regulation and cooperation principles, rather than a handbook to solve all problems.

21. This study is to be seen as a complement to previous Council of Europe documents on this topic, notably the 2017 Council of Europe report on "Information Disorder" [16] (hereafter CoE Information Disorder Report 2017) and the "Study on the use of internet in electoral campaigns" (hereafter CoE Election Study 2017).[17]

III. NEW TECHNOLOGIES AND INFORMATION

22. In online society, information is the prime commodity not only of economic production but also of social interaction and governance. The impact of the internet on reality is universal, and affects even those who have never used the technology. It directly affects public opinion wherever people are located, and

15. See the Reference document CDL-AD(2019)016 for examples of different criteria to solve similar problems.
16. Council of Europe report, DGI(2017)09.
17. Council of Europe study, DGI(2017)11.

has already changed the way that people think and behave in the world around them. It gives voice to each and everyone interested and enables them to contribute to the public discourse, whether negatively or positively. It paves the way for "PR-troops" to rush to the forum when much is at stake to try to influence the turn of events. At times fiction intervenes into this equation with the virtual and the physical.[18] Public figures may discover that their fictional characters are even more influential "actors" than their physical selves.[19] Humor can have a similar effect: Internet users may build different perceptions, by creating fake satirical accounts for public figures for example, which directly affect the image of the person imitated and can sometimes end up confusing the public and the mass media.[20]

23. Information is transmitted mainly through images, which, unlike words, are processed automatically: man risks being converted into a passive receptor, submerged in colours, shapes, sequences and background noises and incapable, in the absence of written culture and verbal language, of transforming information into knowledge, and images into judgments and ideas. This risks resulting in a progressive dilution of the capacity for abstraction. ***Homo sapiens*** [21] is increasingly turning into ***homo videns:*** a creature that looks but does not think, that sees but does not understand. Images are surrounded by written texts, either positive or negative, which are also converted into images and, like other information, are processed in an immediate way, instead of being reflected on.[22]

24. When information is reduced to simple stimuli that affect the recipient,[23] man responds more to persuasion and less to information. The prominence of the image also leads to a difficulty in explaining complex concepts that require a certain level of abstraction. The stimuli to which people respond are almost exclusively audiovisual, with the presumption of truth, and they only react to images that manage to create a reaction. The emotional content in rumors becomes more important than the factual and thus provokes emotional

18. A clear example of the breakdown of the lines of fiction and reality can be observed in DAESH´s communications strategy. By consciously imitating video games and blockbusters, they generate attention, creating a humanized image of the terrorist and a depersonalized image of victims: Lesaca, Javier. Armas de seducción masiva. Peninsula, Atalaya, 2017. By contrast, traditional media do not reflect the consequences of their barbarism in all its harshness.

19. Support for Kevin Spacey, or his incarnation of the President of the United States of America in the series, House of Cards, created a lot of controversy. The case of the wrestler, Hulk Hogan, went to North American courts, and eventually achieved a favourable sentence, based on the distinction between the acts of the fictional character, inside and outside the ring, and the person that represented it.

20. In different social media platforms false accounts are rife, and whether or not they warn of their parodic nature, they create a stereotype of the character that they are imitating, using humour. Some of them end up having more of a following than the real accounts of the person that they are parodying. In Spanish politics, notable examples include @EspeonzaAguirre and @NanianoRajoy.

21. Sartori, Giovanni. Homovidens, Taurus, 1989.

22. In this regard it is important to reconsider the famous phrase by E.M. Foster which said that "Books are facts to be read (which is annoying as that takes a long time); it is the only way of knowing what they contain. Some wild tribes eat them, but in the West reading is the only technique known".

23. Schwartz, Tony. La respuesta emocional. Ed. Liderazgo democrático 2. Quito, 2001. p. 37.

reactions, normally hatred or slander. This is increasingly taken advantage of by PR-agencies paid by political actors to mobilize the ground where hatred and slander have gained foothold.

25. The phenomenon called "fake news"[24] captured popular attention in the wake of the 2016 US presidential elections. "Fake news" describes various distinct phenomena. It usually combines elements of traditional news with features that are exogenous to professional journalism.[25] Fake news is characteristic of the collapse of traditional news (not that disinformation, misinformation or sensationalism are new phenomenons) and the prevailing chaos of social media communication. This is a new version of the old struggle over the definition of truth, political and financial forces waging propaganda wars with "fake news" as the main weapon.

26. The mass distribution of images has decisively contributed to the success of "fake news", by giving information the appearance of infallibility. Communication ends up being converted into a spectacle, rewarding simple concepts, misleading headlines, anything that draws the reader's attention (click bait), although it can end up being reductionist. Form reigns over substance, and images over ideas; there is a search for simple answers that divide the world into black and white, yes and no, and in which there are no nuances. The brevity, the importance of the image and the ease of re-sharing content, typical of social networks, all favor the spread of the techniques that distort reality.

27. Today's expectation for constant updates and even predictions[26] results in information being developed as soon as it is produced, without being checked or reflected upon. This dynamic rewards speed over quality, creating informative cycles that often do not even last twenty-four hours, exhausting information before it has time to be published in the written press the following day. The infinity of storage capacity and its availability means that statements can be recalled in seconds from the respective website months or even years afterwards. These contradictions are also subject to mass diffusion and sometimes, when seen out of context, can be subject to "fake news".

28. Thousands of analyses, opinions and data on each event accumulate in a chaotic way on social networks and are distributed with an almost infinite capillarity through various terminals to which citizens are connected. The overload of information hinders communication, because certain realities manage to go unnoticed, benefitting from the simpler and more eye-catching

24. The Council of Europe Information Disorder report 2017 deliberately refrains from using the term "fake news" on the ground that it is inadequate to capture the complexity of information pollution and has become increasingly politicised.

25. Mourao, R.R. and Robertson, C.T.: Fake News as Discursive Integration: An Analysis of Sites that Publish False, Misleading, Hyperpartisan and Sensational Information, published online: 13 Januar 2019.

26. In Spain, especially on Wikipedia, a current trend involves suggesting that people are dead when they are actually in good health. For example, the nurse who contracted Ebola was cremated and then miraculously came back to life again.

aspects of others. The process of showing facts to correct errors in information is an insufficient means of correcting these errors.

29. Individuals create their own informative ecosystem or personal world, which is formed of auto-referential pieces of information that do not require any type of consistency with earlier texts, nor with reality. The result is a heavily biased perception of those who do not share the same informative ecosystem. The new and varied sources of information allow for the reinforcement of individual ideas and thus give force to confirmation bias, in which attention and credibility are given to information that fuels one´s own beliefs. The algorithms used by personal communication tools and other social networks detect the preferences of users, displaying them more often and thus further reinforcing the knowledge and support of related topics. As such, despite the mass of information available, the majority of it is either not accessed, or accessed by those already convinced of its limited credibility. Undesirable or unwelcome facts can be ignored, in favor of personalized narratives. Information and corrections are selected in order to prove that a particular opinion is correct and that alternative ones are wrong.[27] This can even happen with verified information, as it is shared much more when it reinforces previous ideas than when it questions them.[28]

30. Social environments also determine how information is received, in particular when it allows people to identify with a group and hide what may damage, or not coincide with, the group´s position. The bandwagon effect, for example, is based on the need to belong and the shame of being different. Hence, people trust the opinion of the majority, creating an echo-chamber where opinions are mutually reinforced.

31. The confirmation bias triggers fragmentation between informative bubbles [29] of parallel informative worlds, which makes it difficult for common spaces for debate to exist. The general public sphere is currently being reduced to small highly mobilized blocks isolated from one another. The possibility of communicating and being informed in a selective, almost personalized way, which is principally facilitated through technology and social networks, creates self-referential micro-communities within which the possibility of knowing and putting oneself in the place of the other encourages more radical positions and a lack of dialogue, hindering empathy.[30] Together these two ele-

27. Sunstein, C., Scala, A., Quattrociocchi, W. Echo Chambers on Facebook. 2016. Available at: ssrn.com/abstract= 2795110 (consulted 25/01/2018).

28. Shin, Jieun, Thorson, Kjerstin. Partisan Selective Sharing: The Biased Diffusion of Fact-Checking Messages on Social Media. Journal of Communication. Vol 67, 2017. Available: onlinelibrary.wiley.com/doi/10.1111/jcom.12284/full (consulted 25/01/2018).

29. Parisier, Eli. The filter bubble. The Penguin Press. New York. 2011.

30. Sunstein, C. R. The law of group polarization. Journal of political philosophy 10, 175–195 (2002).

ments promote polarization and allow for the establishment of a single system of values, at least within closed groups that end up silencing and expelling dissidents. As different informative ecosystems interact they often clash, which in itself feeds this polarization, as the credibility of each radical position decreases according to their opposite´s views, again fuelling the radical discourse of the other.[31]

32. Technology does not just affect the way that information is distributed, it affects the entire communicative process of collecting, storing, organizing and distributing information. Citizens are not mere recipients of information, they become major players in the communicative process. They create they own information sources, in the absence of the traditional gatekeepers and regulators. As a result of this abundance and diversity of information, the media loses its referential character and authority. Moreover, the errors made by traditional media sources because of the aforementioned immediacy of the informative process, coupled with the confusion of sources, have furthered the decline of the credibility of the media.[32] In this way individuals join the media, often on equal terms. Personal information spaces are created in which citizens take shelter; faced with floods of content, they have a reduced and manageable, reliable and secure informative universe dominated by relationships with those who are closest to them in their personal and professional lives, and ideological views.

33. As they share information, citizens become the protagonists of communication, questioning the added value of the mass media. The internet is increasingly used by citizens as a source of information,[33] and when they do so, they do not distinguish between the original, more credible, sources of information and the rest of the content from family and friends.[34] In fact 79% view the latter as a credible source of information, followed by the views of academic experts (72%), employees of businesses (60%), and businesses whose services they use (59%). Information from journalists (48%), CEOs (43%), well-known online figures (42%) and celebrities (29%) are at the bottom of the list.[35]

34. The weight that interpersonal communication gains through social networks has led to the mass creation of bots, anonymous, automated and sometimes fake accounts that act as individuals online and increase the massive distri-

31. www.buzzfeed.com/charliewarzel/2017-year-the-internet-destroyed-shared-reality (consulted 25/01/2018).

32. President Trump has used some of these real or apparent failures to award prizes to fake news www.elconfidencial.com/mundo/2018-01-18/trump-fake-news-awards-noticias-falsas-premios_1508101 (consulted 25/01/2018). An example can be consulted at: theintercept.com/2017/12/09/the-u-s-media-yesterday-suffered-its-mosthumiliating-debacle-in-ages-now-refuses-all-transparency-over-what-happened (consulted 25/01/2018).

33. 46% of European Union citizens followed the news on social networks in 2016: Reuters Institute Digital News. Report 2016, available at: reutersinstitute.politics.ox.ac.uk/sites/default/files/research/files/Digital%2520News%2520Report%25202016.pdf (consulted 25/01/2018).

34. According to the report "I saw the news on Facebook" by the Reuters Institute for the Study of Journalism at the University of Oxford, in 2017 over half of British people obtained information from social networks. And of this half, over 50% do not remember the correct information source.

35. Edelman Trust Barometer 2016.

bution of specific information, aiming to create currents of public opinion, acceptance or rejection of people or ideas, in an artificial way.[36] By giving off the impression that they have widespread support, these features create a bandwagon effect, and others accept the ideas shared by this apparent majority. This generates herd behavior, by which individuals neglect personal responsibility and submit themselves to the will of the collective; they imitate one another and deny discrepancy. The redundancy of misinformation, especially when it is found in the mass media, is set up as a "belief", an unquestionable basis whose denial implies the risk of being disqualified.

IV. THE IMPACT OF SOCIAL MEDIA AND THE INTERNET ON DEMOCRACY AND ELECTORAL PROCESSES

35. The internet has given people unprecedented access to information about elections and enabled them to express their opinions, interact with candidates and get actively involved in electoral campaigns.[37] Social media in particular constitute the predominant platform of political debate and, as such, they are sources of political information.[38] Studies suggest that the increasing flux of information fostered by social media strengthen the critical capacity of citizens towards their governments[39] and that there is a strong positive correlation (0.71) between the use of the internet and social media, on one side, and the support to democracy as a desirable form of government, on the other.[40] Moreover, many authors argue that the generalised use of internet and social media provides a more accurate knowledge of the citizens' interests and facilitates the organisation of large scale social movements.[41]

36. Nonetheless, even if "[t]he internet has the power to be a tool of democracy… its potential in this respect is at risk… [because the] same technology that facilitates discourse creates opportunities for censorship of information, monitoring of online practices and the subtle shaping and manipulation of behaviour",[42] hence threatening the authenticity of suffrage, the equity of the electoral competition and, ultimately, the capacity to translate the ***will of the people*** into institutional representation and governmental decisions.[43] It should be noted that any undue influence over the authenticity and freedom of suffrage might affect not only the translation of the popular will into concrete actions, but also the protection of minorities, the balance among basic human rights and the possibility to hold political parties and elected officials

36. agendapublica.elperiodico.com/desde-rusia-bots.
37. CoE Election Study 2017, p. 7.
38. Democracy Reporting International 2017.
39. Gainous et al. 2016.
40. Basco 2018.
41. Castells 2011; Metaxas and Mustafaraj 2012; Cohen et al. 2012; European Union 2015.
42. Laidlaw 2015, p. 1.
43. Cf. CoE Election Study 2017, p. 7-9. See also Tambini 2018, p. 265-293.

accountable. Even if such threats already existed in the past, they have increased through the more sophisticated methods facilitated by digital technologies.

37. The constant and simultaneous flux of information in real time across multiple platforms represents a huge challenge for the surveillance of behaviour and resources during political campaigns. Moreover, the scattered and anonymous creation of content seriously hampers the identification and attribution of responsibilities for illegal online behaviours. The growing use of ***bots*** and ***trolls*** to set agenda in the social media, as well as the massive distribution of false information, seriously damage the equity in the electoral competition and allow for external actors to manipulate the discourse and the voting preferences.[44] Furthermore, the algorithms that govern search engines and social media may foster a partial and sometimes illusory comprehension of politics and democracy.[45]

38. The impact of the digital environment on elections was highlighted in the controversies following the United Kingdom Brexit referendum and the United States presidential elections in 2016. The enforcement of rules and regulations on paid advertising was limited; voters' personal data were collected and processed for election purposes without their consent and in lack of legal entitlement; political communication was channeled to unregulated social media platforms without safeguards in place on fair media coverage. These implications challenged the established institutions and principles of regulation of election communications such as freedom of association, spending limits and regulation of political advertising,[46] and undermined the ability of the current regulatory regimes to maintain a level playing field in electoral communication. They posed threats to elections and unleashed a potential for corrupt practices to emerge.

39. The transformed communicative spheres on the internet and the changed way of transmitting political messages to voters making it possible for false and/or harmful information to "spread among potential voters on an unprecedented scale without any oversight or rebuttal".[47] This has led to a degree of ***information disorder***, which may take three different forms:

    - Mis-information, that is sharing false information, but without the intent of causing harm;
    - Dis-information, which stands for knowingly sharing false information with the intent to harm; and
    - Mal-information, which describes genuine information shared with the

44. Quintana 2016; Fidler 2017.
45. Van Dijck 2013; McChesney 2013.
46. CoE Election Study 2017, p. 13.
47. CoE Election Study 2017, p. 15.

intent to cause harm, often by disclosing information from the private sphere into the public sphere.[48]

40. In certain cases untrue information has been *strategically* disseminated with the intent to ***influence election results***. It has been documented that ***cyber troops*** on the internet are often ***government, military or political party teams committed to manipulating public opinion*** over social media. Organised ***social media manipulation first emerged*** in 2010, and by 2017 there are details on such organisation s in 28 countries.[49]

41. Not only the social media, but also search engine providers can manipulate information with or without the intent to skew the election results in favour of a particular political option. Recent research shows that manipulations of search results by those providers can produce a so-called ***search engine manipulation effect*** which can shift the voting preferences of undecided voters by 20% or even more in some demographic groups.[50]

42. There are cases where state agencies have employed armies of "opinion shapers" to spread government views and counter critics on social media, or the case of Cambridge Analytica, the company that is being investigated for its alleged role in the 2017 US presidential elections and in the Brexit referendum for accessing and using private data of 50 million Facebook users.[51] Unlike other direct methods of censorship, such as website blocking or arrests for internet activity, online content manipulation is difficult to detect and even more difficult to defeat, given its dispersed nature and the sheer number of people and bots employed for this purpose.

43. As targeted messages do not reach the public, but only selected groups or individuals, and are not subject to any oversight or journalistic scrutiny, political candidates and parties can make different promises to different people, dispersing their political objectives into separate, not necessarily reconcilable messages. Indeed, some research shows increased digital campaigning on the so-called wedge issues, those that are highly divisive but have the ability to mobilise voters (immigration policies, welfare, same-sex marriages, etc.). Lastly, message targeting seeks to optimise the electoral campaigns' resources and thus focuses largely on swing or undecided voters. Those who are not singled out by political party messages are deprived of an entire spectrum of political stances, which in turn creates inequalities in terms of the available information on which the voters base their political choices.

48. CoE Information Disorder Report 2017.

49. Bradshaw & Howard, 2017. See also the Freedom House 2017 report, according to which manipulation and disinformation tactics played an important role in elections in at least 17 other countries over the year. According to the Communications Security Establishment (CSE) of the Government of Canada, in 2017 alone, 13% of countries holding federal elections have had their democratic process targeted by hacktivist, cybercriminals, and even public or private political actors, all of them with the intent to manipulate information, sway public opinion or even destabilise democratic institutions.

50. Epstein & Robertson, 2015.

51. Mccausland, P. and Schecter, A., 2018, BBC, 2018.

44. Finally, states and private actors all over the world can use the digital technologies to violate human rights or even as a military instrument to attack countries and their institutions through malware, ransom ware, spyware and other sophisticated programmes.[52] This is known as "***cyber warfare***" and has been previously and successfully used to undermine state projects and systems, for instance the Stuxnet attack on the Natanz (Iran) nuclear plant.[53]

45. Along with their accessibility, sophistication and public appeal, cybernetic tools are embedded in a borderless environment. What was legally created under national laws, could now be illegally allocated in a different jurisdiction or vice versa. Moreover, with the increasing use of ***cloud computing***, the online information has become even more fragmented, thus making it extremely difficult to identify its origin or authorship. Cybercrime and cyber-threats operate beyond the limits of any national jurisdiction. This situation presents several difficulties to criminal investigation and prosecution; hence, the urge to attend this phenomenon from a transnational perspective.[54]

46. To conclude, today we are witnessing the parallel proliferation of information and its pollution at a global scale. The internet-based services have enriched and diversified news sources, facilitating individuals' access to information and their decisions on the most crucial matters in democracy, notably on the choice of their legislature. However, at the same time, a new era of information disorder distorted the communication ecosystem to the point where voters may be seriously encumbered in their decisions by misleading, manipulative and false information designed to influence their votes. This environment potentially undermines the exercise of the right to free elections and creates considerable risks to the functioning of a democratic system.

47. Digital technologies have reshaped the ways in which societies translate the will of the people into votes and representation, and they have to a large extent changed political campaigning. Even though the internet fosters some aspects of the democratic contest, it also hampers them. The worldwide pervasiveness of digital technologies has moved the arena of democratic debate to the virtual world, raising many questions about their influence on voter turnout and the need to survey and regulate online social behaviour. Moreover, adequate protection against cyber warfare needs to be ensured.

V. RELEVANT EUROPEAN AND INTERNATIONAL STANDARDS AND INSTRUMENTS

48. The aforementioned phenomena interfere with a number of fundamental rights protected at European and universal level by several international declarations and conventions, such as the Universal Declaration of Human

52. Quintana 2016.
53. Quintana 2016; Mecinas Montiel 2016, p. 404, 418-419.
54. Davara 2003; Salt 2017 p. 520-521.

Rights, the International Covenant on Civil and Political Rights, the American Declaration of the Rights and Duties of Man, the American Convention on Human Rights, the Charter of Fundamental Rights of the European Union and the European Convention on Human Rights (hereafter ECHR).

A. RIGHT TO FREE ELECTIONS AND FREEDOM OF EXPRESSION

1. Basic principles

49. Under the ECHR, as interpreted by the European Court of Human Rights (hereafter the ECtHR), the Council of Europe member states have an obligation to secure the rights and freedoms for everyone within their jurisdiction. The ***right to free elections*** enshrined in Article 3 of Protocol No. 1 to the ECHR is not only an objective and essential principle in any democratic society, but also a fundamental individual right on which every citizen can rely, one that most effectively promotes "true democracy".[55]

50. The right to free elections incorporates the right to vote and the right to stand for election.[56] Moreover, it also entails a positive obligation on the member states to ensure conditions under which people can freely form and express their opinions and choose their representatives. This obligation is of utmost importance with regard to the (un)disrupted communicative context of elections. The right to free elections provides that member states "undertake to hold free elections at reasonable intervals by secret ballot, under conditions which will ensure the free expression of the opinion of the people in the choice of the legislature", which indicates that the rights to freedom of expression and to free elections are prerequisites of each other.[57] This interpretation was reaffirmed by the ECtHR in stating that "free elections and freedom of expression, particularly freedom of political debate, together form the bedrock of any democratic system".[58]

51. The ECtHR further stated that the two rights are inter-related and operate to reinforce each other, freedom of expression being one of the conditions necessary to ensure free elections. In order for the rights guaranteed by Article 3 of Protocol No. 1 to be effective, their protection extends to the election campaign. For this reason, it is particularly important in the period preceding an election that opinions and information of all kinds are permitted to circu-

55. Thorgeirsdóttir, Herdis (2005), Journalism Worthy of the Name: the Affirmative Side of Article 10 of the ECHR, Kluwer Law International. Lécuyer, 2014. See Mathieu-Mohin and Clerfayt v. Belgium, Application no. 9267/81 (ECtHR, 2 March 1987); Ždanoka v. Latvia, Application no. 58278/00 (ECtHR, 16 March 2006). See also ECtHR, 2018, "Guide on Article 3 of Protocol No. 1 to the European Convention on Human Rights – Right to free elections", available at: www.echr.coe.int/Documents/Guide_Art_3_Protocol_1_ENG.pdf

56. Mathieu-Mohin and Clerfayt v. Belgium; Ždanoka v. Latvia.

57. Plaizier, 2018.

58. Bowman v the United Kingdom, Application no. 24839/94 (ECtHR, 19 February 1998), para 42.

late freely.[59] According to the ECtHR, member states have a positive obligation to ensure the effectiveness of freedom of expression: they are required to create a favourable environment for participation in public debate by all persons concerned, enabling them to express their opinions and ideas without fear. The state must not just refrain from any interference in the individual's freedom of expression, but is also under a positive obligation to protect his or her right to freedom of expression against attack, including by private individuals.[60]

52. The ECtHR recognised however that in certain circumstances the rights under Article 10 ECHR and Article 3 of Protocol No. 1 may conflict and it may be considered necessary, in the period preceding or during an election, to place certain restrictions on freedom of expression, of a type which would not usually be acceptable, in order to secure the "free expression of the opinion of the people in the choice of the legislature".[61] The Court recognised that, in striking the balance between these two rights, member states have a margin of appreciation, as they do generally with regard to the organisation of their electoral systems. At the same time, it stressed that any restrictions on freedom of expression must be proportionate to the legitimate aim pursued and necessary in a democratic society. The Court indicated for example that Article 10 ECtHR as such does not prohibit discussion or dissemination of information received even if it is strongly suspected that this information might not be truthful.[62] On the other hand, attention is drawn to the Court's decision concerning the right of an NGO to make political advertisements on radio and television, in which it balanced the applicant NGO's right to impart information and ideas of general interest which the public is entitled to receive with the authorities' desire to protect the democratic debate and process from distortion by powerful financial groups with advantageous access to influential media.[63] The Court recognised that such groups could obtain competitive advantages in the area of paid advertising and thereby curtail a free and pluralist debate, of which the state remains the ultimate guarantor. As a result, the risk of an imbalance between political forces in competition has to be taken into account to maintain a free and pluralist debate.

53. The rights under Article 3 of Protocol No. 1 are not absolute either: there is room for "implied limitations",[64] and the member states must be given a wide

59. Bowman v the United Kingdom, Application no. 24839/94 (ECtHR, 19 February 1998); Orlovskaya Iskra v. Russia, Application no. 42911/08 (ECtHR, 21 February 2017). During the 2019 European elections, Facebook allowed EU-wide political ads for the European Parliament: www.politico.eu/article/facebook-allows-euwide-political-ads-for-european-parliament/; techcrunch.com/2019/04/26/facebook-says-its-open-toadvertising-u-turn-for-the-eu-elections-enabling-cross-border-campaigns/?renderMode=ie11.

60. Dink v. Turkey, Application no. 2668/07, 6102/08, 30079/08, 7072/09 and 7124/09 (ECtHR, 14 September 2010).

61. Bowman v the United Kingdom, Application no. 24839/94 (ECtHR, 19 February 1998); Orlovskaya Iskra v. Russia, Application no. 42911/08 (ECtHR, 21 February 2017).

62. Salov v. Ukraine, Application no. 655118/01 (ECHR, 6 September 2005).

63. Animal Defenders International v. the United Kingdom, Application no. 48876/08 (ECHR, 2013).

64. Article 3 is not limited by a specific list of "legitimate aims" such as those enumerated in Articles 8 to 11 ECHR, and the ECtHR does not apply the traditional tests of "necessity" or "pressing social need" which are used in the context of Articles 8 to 11 ECHR.

margin of appreciation in this sphere. In examining compliance with Article 3 of Protocol No. 1, the Court has focused mainly on two criteria: whether there has been arbitrariness or a lack of proportionality, and whether the restriction has interfered with the free expression of the opinion of the people.[65]

54. The ECtHR recognised the right of individuals to access the internet, as in its ruling against the wholesale blocking of online content, it asserted that "the internet has now become one of the principal means of exercising the right to freedom of expression and information, providing as it does essential tools for participation in activities and discussions concerning political issues and issues of general interest".[66] It stated that Article 10 ECHR guarantees the freedom to express, receive and impart information and ideas regardless of frontiers. Blocking access to host and third-party websites in addition to websites concerned by proceedings renders much information inaccessible, thus restricting the rights of internet users. The Court further clarified that a restriction on access to a source of information is only compatible with the Convention if a strict legal framework, affording the guarantee of judicial review to prevent possible abuses, is in place.

55. Moreover, the ECtHR acknowledged that "given the important role played by the internet in enhancing the public's access to news and facilitating the dissemination of information (see Delfi AS v. Estonia [GC], § 133, ECHR 2015), the function of bloggers and users of the social media may be assimilated to that of "public watchdog" in so far as the protection of Article 10 is concerned".[67] This protection may extend to access to (publicly held) information if it is instrumental for the exercise of the right to freedom of expression: the information to which access is sought must meet a public-interest test. Nonetheless, as mentioned earlier, Article 10 does not guarantee an unlimited freedom of expression; restrictions may be permitted, for example, in order to protect the right to private life (Article 8 ECHR), if the means used are proportionate to the aim pursued.

56. Fundamental principles relating to elections are furthermore expressed in the Code of Good Practice in Electoral Matters adopted by the Venice Commission in 2002.[68] They include, ***inter alia***:

- equality of opportunity for parties and candidates;
- a neutral attitude by state authorities with regard to the election campaign, to coverage by the media, and to public funding of parties and campaigns;

65. Mathieu-Mohin and Clerfayt v. Belgium; Ždanoka v. Latvia.

66. Ahmet Yıldırım v. Turkey, Application no. 3111/10 (ECtHR, 18 December 2012). See also Cengiz and Others v. Turkey, Application nos. 48226/10 and 14027/11 (ECtHR, 1 December 2015).

67. Magyar Helsinki Bizottság v. Hungary, Application no. 18030/11 (ECtHR, 8 November 2016). See also Animal Defenders International v. the United Kingdom, Application no. 48876/08 (ECHR, 2013).

68. CDL-AD(2002)023rev-cor. See also the Joint Guidelines for Preventing and Responding to the Misuse of Administrative Resources during Electoral Processes (CDL-AD(2016)004), which reaffirm the principles of neutrality and equality of opportunity concerning access to publicly-owned media.

- equality of opportunity can be proportional rather than strict, and applies in particular to "radio and television air-time";
- in conformity with freedom of expression, legal provision should be made to ensure that there is a minimum access to privately owned audio-visual media, with regard to the election campaign and to advertising, for all participants in elections;
- campaign funding must be transparent;
- equality of opportunity can lead to a limitation on political party spending, especially on advertising.

57. The basic principles relating to elections are subject to particular challenges when electronic voting methods are used. The Council of Europe continues to be the only organisation that has set intergovernmental standards in the field of e-voting. The Committee of Ministers Recommendation Rec(2004)11, which has been used in national jurisprudence even in non-member states, as well as by other relevant international actors, has recently been updated: a new recommendation – which consists of the actual Recommendation CM/Rec (2017)5 on standards for e-voting, the guidelines on the implementation of the provisions of the Recommendation with specific requirements and the Explanatory Memorandum – was drafted as an enhancement of Rec(2004)11 and deals with the most critical part of election technology, namely e-voting, which means the use of electronic means to cast and count the vote. This category includes systems such as Direct Recording Electronic (DRE) voting machines, ballot scanners, digital pens and internet voting systems. The Recommendation is aimed at ensuring that e-voting guarantees universal, equal, free and secret suffrage, and it includes provisions on organisational requirements, accountability, reliability and security of the system.

58. In this connection, attention is also drawn to relevant Venice Commission documents. The Code of Good Practice in Electoral Matters makes it clear that "electronic voting should be used only if it is safe and reliable; in particular, voters should be able to obtain a confirmation of their votes and to correct them, if necessary, respecting secret suffrage; the system must be transparent".[69]

2. Funding of electoral campaigns

59. There is a range of commonly agreed standards against corruption in the funding of political parties and electoral campaigns (which are recommended to also apply to entities related to political parties, such as political foundations). They were set by the Parliamentary Assembly Recommendation 1516 (2001) on the financing of political parties and followed upon by the Committee of Ministers Recommendation Rec(2003)4 on common rules against corruption in the funding of political parties and electoral campaigns. The

69. Code of Good Practice in Electoral Matters, CDL-AD(2002)023rev-cor, section I.3.2.IV.; see also paragraphs 42-44 of the Explanatory Memorandum. See also the Venice Commission Report on the compatibility of remote voting and electronic voting with the standards of the Council of Europe, CDL-AD(2004)12.

standards to be applied include (a.) requirements on a ***reasonable balance*** between public and private funding of political parties; (b.) the use of ***fair criteria*** for the distribution of state contributions to parties; (c.) imposition of strict rules concerning private donations including ***bans on or limitations of contributions*** from foreign donors, religious organisations and restrictions on corporations and anonymous donations; (d.) ***limitations on parties' expenditures*** linked to election campaigns; (e.) provisions on ***transparency*** of donations and expenses of political parties; and (f.) the establishment of an ***independent authority*** and meaningful ***sanctions*** for those who violate the rules.

60. Similarly, in the Guidelines on Political Party Regulation,[70] the Venice Commission and OSCE/ODIHR set out that electoral campaigns' regulations should

- prevent improper influence (and ensure the independence of parties) on political decisions through financial donations;
- provide for transparency in expenditure of political parties and
- ensure that all political parties have an opportunity to compete in line with the principle of equal opportunity.

61. In order to achieve these objectives, the "main ways campaign communication has been regulated has been through electoral law including spending limits and campaign finance controls; subsidies for campaigning communications; pre-poll black outs; media regulation in particular broadcast licensing; rules on political advertising including impartiality, subsidies and free air time; and self-regulation and journalism ethics".[71]

62. The applicable standards were set high in order to "protect the integrity of elections, ensure they are free and fair, and not captured by a narrow range of interests."[72] However, the legislative steps taken by the member states and regulations implemented focused on the offline context.[73] Therefore, their ***applicability and efficacy in times of digital political advertising*** turned out to be ***severely limited***. As mentioned earlier, in recent years policy-makers, governments and civil society alike had to face the reality of there being limits to ***law enforcement of the current regulation on the internet***, including as regards the applicability of existing regulation on electoral campaigns.

63. Namely, legislative limits on campaign finance have been challenged by new forms of digital advertising which are inherently less transparent than their analogue predecessors, thus undermining the existing definitions and restrictions based on specific media types. The safeguards against corruption based on methods for calculating spend and categories for reporting spend

70. CDL-AD(2010)024, p. 35, para. 159.
71. CoE Election Study 2017, p. 9.
72. CoE Election Study 2017, p. 9.
73. In this context, the use of crowd funding campaigns, mainly through the internet, is increasingly important in changing the scope of funding for electoral campaigns.

on traditional media channels have lost their meaning as political campaigning shifted to the internet. As a result, also the absolute spending limits imposed on broadcasting are becoming less meaningful, while transparency regulations ensuring that citizens are aware of campaign finance and spend are difficult, if not impossible to implement across borders in the digital environment.[74]

3. Political speech and media coverage on electoral campaigns

64. While "freedom of expression is the lifeblood of democracy", all legal systems now have campaign funding rules and limits and transparency obligations. In the individual sphere it may be that the expression deserves protection irrespective of content, but that does not apply to a campaign. The vast majority if not the totality of the constitutional systems contemplate limits on freedom of expression during an election campaign: for instance, the silence period, cordon sanitaire at polling stations, campaign funding rules and transparency obligations. All campaign restrictions, even those promoting transparency, must be seen firstly as an interference which must be justified, in European systems, according to a test of necessity and proportionality. Regulating the publication of political advertising seems legally possible in the principle for a) Regulation on transparency rather than content, b) regulation on political campaigning, c) Regulation which is either aimed at elections or polls or linked to funding mechanisms or aimed to identify an origin outside the political community. While there are difficult concepts to pin down it is clearly possible to design a scheme for traditional press, broadcasting or poster advertising. But in the digital sphere what is publication and who is the publisher? When is a message "advertising" rather than the individual expression of opinion which "goes viral"?

65. The ECtHR has clearly pointed to the responsibility of the state for preventing inequality in media coverage during elections[75] online and offline, however with significant differences as regards the ***influence*** between traditional media and new media.[76] The issue at stake now is how to define those differences precisely – ***whether they have already reached a "sufficiently serious shift in the respective influence".***[77] The crucial caption of the momentum of this "shift" is to determine whether the positive responsibility of the state in assuring equal exposure of political parties and candidates are to be applied to new information intermediaries and in what manner.

66. The Council of Europe standards and other instruments in this area seek to provide an ***enabling communication context for the enjoyment of the right to free elections.*** They reflect the positive obligations of the state to ensure that citizens receive necessary and truthful information on political parties to support their democratic choice to elect their representatives.

74. CoE Election Study 2017, p. 20-21.
75. Communist Party of Russia and Others v Russia App. no. 29400/05 (ECtHR, 19 June 2012).
76. Animal Defenders International v the United Kingdom App. no. 48876/08 (ECtHR, 22 April 2013).
77. Ibid., para 119.

67. Recommendation CM/Rec(2007)15[78] applies to a broad range of media, irrespective of the means and technology used for the dissemination of their content, providing guidelines for free and independent media coverage of political campaigns, with higher standards applicable to the public service media outlets. The Recommendation includes a number of guidelines aimed at ensuring responsible, accurate and fair coverage of electoral campaigns; however public service media have a particular responsibility to cover elections in a "fair, balanced and impartial manner, without discriminating a specific political party or a candidate". As regards the overall opportunities for the political parties and candidates to address the electorate, the Recommendation leaves it to the discretion of individual member states whether they will allow for paid political advertising. However, where parties have the possibility of buying advertising space for the purpose of electoral campaigning, they must be able to do so under equal conditions and rates of payment.

68. Furthermore, the Recommendation sets out a few general requirements for ensuring fair and transparent campaigns; for example, the ***right of reply*** or equivalent remedies should be made available to the candidates and/or political parties, so as to enable them to effectively respond to any statements that might cause them prejudice during the relatively short duration of electoral campaigns. Also, the ***modalities of disseminating opinion polls*** should provide the public sufficient information to make a judgment on the value of the polls, while the potential impact of electoral messages just before the elections is mitigated by the provision allowing the member states to consider prohibiting their dissemination on the day preceding voting ("day of reflection"). Moreover, the Recommendation spells out ***transparency requirements*** on ***paid advertising content*** along with ***ownership*** of the outlets (these requirements are detailed by Recommendation CM/Rec(2018)1).[79] The above-mentioned guidelines target, first and foremost, linear broadcast (private and public) media with extensions to non-linear audiovisual services of public service media. However, with the shift of political campaigning to the online social media context in the past decade, their effectiveness is proving to be reduced.

69. This shift is reflected also in Recommendation CM/Rec(2018)1 which clearly points to the potentially disturbing impact that the online platform's control over the flow, availability, findability and accessibility of information can have on ***media pluralism***. Selective exposure to media content leading to potential societal fragmentation is identified as one of the major concerns especially during the time of elections. Therefore, the Recommendation calls on the states to fulfill their positive responsibility and to act as the ultimate guarantor of media pluralism by ***ensuring pluralism in the entirety of the multimedia ecosystem.***

78. Recommendation CM/Rec(2007)15 of the Committee of Ministers to member states on measures concerning media coverage of electoral campaigns.

79. Recommendation CM/Rec(2018)1 on media pluralism and transparency of media ownership.

70. This interpretation is reinforced by Recommendation CM/Rec(2018)2[80] which addresses the roles and responsibilities of internet intermediaries in relation to their users and to the member states, having due regard to their growing power over communication and the dissemination of information. The potential coresponsibility of intermediaries for content that they store - if they do not act expeditiously to restrict access to content or services as soon as they become aware of their illegal nature (in line with the principles of legality, necessity and proportionality) - should be read in this context. Meanwhile, intermediaries should bear no general obligation to monitor content, which they merely give access to, or which they transmit or store. In this connection, attention is also drawn to the Recommendation CM/Rec(2016)1 which calls on member states to safeguard the principle of network neutrality in the development of national legal frameworks, in order to ensure the protection of the right to freedom of expression and to access to information, and the right to privacy.[81]

71. In its Declaration Decl(13/02/2019)1 of 13 February 2019 on the manipulative capabilities of algorithmic processes, the Committee of Ministers emphasised "the need to assess the regulatory frameworks related to political communication and electoral processes to safeguard the fairness and integrity of elections offline as well as online in line with established principles. In particular it should be ensured that voters have access to comparable levels of information across the political spectrum, that voters are aware of the dangers of political redlining, which occurs when political campaigning is limited to those most likely to be influenced, and that voters are protected effectively against unfair practices and manipulation."

72. The Parliamentary Assembly in its Resolution 2254 (2019)[82] on Media freedom as a condition for democratic elections[83] called on member states to implement effective strategies to protect the electoral process from the information manipulation and undue propaganda through social media. It proposed measures such as the development of specific regulatory frameworks for internet content at election times, and the establishment of a clear legal liability for the social media companies that publish illegal content harmful to candidates – while avoiding extreme measures such as the blocking of entire websites. The Parliamentary Assembly further called on organisations in the media sector to develop self-regulation frameworks with professional and ethical standards for their coverage of election campaigns, and on internet intermediaries to co-operate with civil society and organisations of all political affiliations specialising in the verification of content, to ensure that all information is confirmed by an authoritative third-party source.

80. Recommendation CM/Rec(2018)2 on the roles and responsibilities of internet intermediaries.
81. Recommendation CM/Rec(2016)1 on protecting and promoting the right to freedom of expression and the right to private life with regard to network.
82. Declaration Decl(13/02/2019)1 on the manipulative capabilities of algorithmic processes, search.coe.int/cm/pages/result_details.aspx?ObjectId=090000168092dd4b.
83. Resolution 2254 (2019) on Media freedom as a condition for democratic elections assembly.coe.int.

B. RIGHT TO PRIVACY AND PERSONAL DATA PROTECTION

73. Article 8 ECHR provides for the protection of the right to privacy. On this basis, the ECtHR has developed extensive case law concerning personal data protection.[84]

74. The Council of Europe Convention on the protection of individuals with regard to automatic processing of personal data ETS No. 108 of 1981 sets out principles and rules for personal data processing as well as the rights of individuals. The Additional Protocol to the Convention of 2011 sets standards for the establishment of data protection supervisory authorities. The particular added value of this legal framework in comparison with the European Union General Data Protection Regulation is that, being open to any country in the world, it allows various legal systems to stand under the same umbrella, hence, harmonising different legal regimes.[85]

75. On 10 October 2018 the new protocol modernising this Convention (hereafter the Modernised Convention) was signed by 21 of the Parties to the Convention. Article 5 of the Modernised Convention strengthens the data protection principles by requiring that data shall be processed fairly and in a transparent manner, collected for explicit, specified and legitimate purposes and not processed in a way incompatible with those purposes, while any further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is subject to appropriate safeguards, compatible with those purposes. The Modernised Convention furthermore provides for additional principles and requirements such as privacy by design, personal data impact assessment and privacy by default, as well as the compulsory notification of data breach to, at least, data protection authorities. It introduces additional safeguards, in particular having in mind the omnipresence of information technologies in data processing, and recognises new categories of data as of sensitive nature. The additional safeguards particularly apply to the processing of sensitive data such as political opinions. The Modernised Convention provides for more detailed provisions on transborder data flows, on additional requirements on data controllers and on the follow-up mechanism.

76. In addition, there are a significant number of Council of Europe legal instruments pertaining to the protection of personal data within the operation of social networks.

77. The 1999 Committee of Ministers Recommendation No. R (99) 5 for the protection of privacy on the internet includes Guidelines for the protection of

84. Case law of the ECtHR concerning the protection of personal data, available at: rm.coe.int/case-law-ondata-protection/1680766992. See also ECtHR, 2018, "Guide on Article 8 of the European Convention on Human Rights – Right to respect for private and family life", available at: www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf.

85. This concerns both non-European countries (Cabo Verde, Mauritius, Mexico, Senegal, Tunisia and Uruguay) and European countries (e.g. Albania, Russia, Serbia, Turkey, Ukraine).

individuals with regard to the collection and processing of personal data on information highways. The 2010 Recommendation CM/Rec(2010)13 on the protection of individuals with regard to automatic processing of personal data in the context of profiling provides for conditions for such processing and sets out a detailed list of information needed to be given to data subjects. It notes that the lack of transparency, or even "invisibility", of profiling and the lack of accuracy that may derive from the automatic application of pre-established rules of inference can pose significant risks for the individual's rights and freedoms. Although initially perceived as a technique used in a business and marketing context, the recent events demonstrate that profiling is also applied in the election processes.

78. The 2010 Ministers of Justice Resolution No. 3 on data protection and privacy in the 3rd millennium, MJU-30 (2010) RESOL, notes probable consequences of the wide use of ICTs enabling observation, storage and analysis of most day-to-day human activities, thereby potentially inducing a chilling effect linked to the feeling of being under surveillance, which may impair the free exercise of human rights and fundamental freedoms unless robust standards of data protection are effectively enforced worldwide. The 2011 Parliamentary Assembly Resolution 1843 (2011) on the protection of privacy and personal data on the internet and online media emphasises that the protection of the right to data protection is a necessary element of human life and of the humane functioning of a democratic society, and that its violation affects a person's dignity, liberty and security.

79. The 2012 Committee of Ministers Recommendation CM/Rec(2012)3 on the protection of human rights with regard to search engines recognises the challenge caused by the fact that an individual's search history contains a footprint which may reveal the person's beliefs, interests, relations or intentions, and could reveal, ***inter alia***, one's political opinions or religious or other beliefs. It calls for action to enforce data protection principles, in particular purpose limitation, data minimisation and limited data storage, while data subjects must be made aware of the processing and provided with all relevant information.

80. Recommendation CM/Rec(2012)4 on the protection of human rights with regard to social networking services notes the increasingly prominent role of such and other social media services, offering great possibilities for enhancing the potential for the participation of individuals in political, social and cultural life. It recommends actions to provide an environment for users of social networks that allows them to further exercise their rights and freedoms, to raise users' awareness of the possible challenges to their human rights and of the negative impact on other people's rights when using these services, as well as to enhance transparency about data processing, and to forbid the illegitimate processing of personal data. These actions may be taken by engaging with social networking providers. The Recommendation also underlines that users should be informed where their personal data is used in the context of profiling.

81. The 2013 Committee of Ministers Declaration on Risks to Fundamental Rights stemming from Digital Tracking and other Surveillance Technologies stresses that member states do not only have the negative obligation to refrain from interference with human rights, but also the positive responsibility to actively protect these rights, which includes the protection of individuals from action by non-state actors. The ubiquitous use of various devices and information gathered through those devices make tracking and surveillance of people possible, thus revealing delicate and/or sensitive personal information, including political or religious preferences, which can be aggregated to provide detailed and intimate profiles of them.

82. The 2014 Committee of Ministers Recommendation CM/Rec(2014)6 provides for a Guide to human rights for internet users, and in 2017 the Committee of Convention ETS 108 adopted Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data. In its Declaration Decl(13/02/2019)1 of 13 February 2019 on the manipulative capabilities of algorithmic processes, the Committee of Ministers encouraged member states to "consider the need for additional protective frameworks related to data that go beyond current notions of personal data protection and privacy and address the significant impacts of the targeted use of data on societies and on the exercise of human rights more broadly".

83. Finally, the Council of Europe produced or commissioned different reports and studies in the field, including the Report on "the use of the Internet & related services, private life & data protection: trends & technologies, threats & implications".[86] The latter calls for affirming and protecting the right to anonymity on the internet, regulating and strictly limiting the creation and use of profiles, in all kinds of different contexts, and for the adoption by the Council of Europe of guidelines on the restrictions to be imposed on surveillance technologies, including the international trade in such technologies.

C. PROTECTION AGAINST CYBERCRIME

84. The Council of Europe Convention on Cybercrime ETS 185 of 2001 ("Budapest Convention") addresses two types of threats to electoral democracy.[87] Firstly, attacks against the confidentiality, integrity and availability of election computers and data, which represent forms of cybercrime such as illegal access to computer systems (Article 2), illegal interception (Article 3), data and system interference (Articles 4 and 5) and others. Secondly, dis-information operations where rules on the protection of personal data, on political finances, on media coverage or on the broadcasting of elections, that is, rules to ensure free, fair and clean elections, are violated.

86. Korff, 2013, at rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168067f7f4_86

87. The following information is based on a presentation by Alexander Seger (Executive Secretary, Cybercrime Convention Committee, Council of Europe) at the 15th European Conference of Electoral Management Bodies, Oslo, Norway, 19-20 April 2018.

85. While the second type of conduct does not constitute cybercrime per se, the evidence that such rules are broken often takes the form of electronic evidence. It is essential, therefore, that states provide their criminal justice authorities with the necessary powers to secure such evidence. Parties to the Budapest Convention are required to do so under Articles 16 to 21 that cover procedural law powers such as the expedited preservation of data, the search and seizure of computer systems and data, production orders and others.

86. A major problem is that data – and thus electronic evidence – is volatile and often held by service providers in foreign jurisdictions or stored in multiple, shifting or unknown jurisdictions, that is, "somewhere on servers in the cloud".[88] Attributing an attack, or simply identifying the user of an Internet Protocol (IP) address or the owner of a social media or email account is often not possible with reasonable effort. This is one of the reasons why cybercrime and other cyber threats to electoral democracy are rarely prosecuted.

87. Effective international cooperation and cooperation with service providers is warranted. The Budapest Convention in its current form includes detailed provisions on international cooperation combining expedited provisional measures to secure data (e.g. Article 29 on expedited preservation and Article 35 on 24/7 points of contact) with provisions on mutual legal assistance. These provisions are routinely used to investigate cybercrime.

88. However, these do not sufficiently address the problem of cloud computing and related problems of jurisdiction or the fact that service providers in one state offer their services in many others without being legally or physically present or accountable in the latter.

89. For this reason, the Parties to the Budapest Convention have launched the negotiation of a 2nd Additional Protocol to permit added options for enhanced international cooperation and access to data in the cloud. Solutions under consideration include direct cooperation with service providers in other Parties, extending searches to computers in other jurisdictions in limited circumstances, or emergency mutual assistance. Negotiations are expected to last until the end of 2019.[89]

VI. OTHER INTERNATIONAL AND NATIONAL LEGISLATION, CASE LAW AND INITIATIVES [90]

A. INTERNATIONAL LEVEL

90. At the level of the United Nations, it was noted in the Joint Declaration on Freedom of Speech and Internet of 1 June 2011[91] that the approaches to

88. For detailed background information see the reports prepared by the Cloud Evidence Group on the Cybercrime Convention Committee, www.coe.int/en/web/cybercrime/ceg (last accessed 30 September 2018).

89. See www.coe.int/en/web/cybercrime/t-cy-drafting-group.

90. This report does not contain an exhaustive description of national material. See also CDL-AD(2019)016.

91. Declaration signed by the UN Special Rapporteur on Freedom of Opinion and Expression, OSCE Representative on Freedom of the Media, OAS Special Rapporteur on Freedom of Expression and ACHPR Special Rapporteur on Freedom of Expression and Access to Information on 1 June 2011.

regulation developed for other means of communication – such as telephone services or broadcasting – are very different to the ones needed for the internet, and such methods must be specifically designed for it. The more recent Joint Declaration, of 3 March 2017, now includes "fake news", disinformation and propaganda, and underlines the necessity to prioritise the freedom of speech, stating that the prohibitions on the dissemination of information based on vague and ambiguous ideas, including "false news" or "non-objective information", are incompatible with international standards for restrictions on freedom of expression, as set out in paragraph 1(a),[92] and should be abolished.

91. Growing awareness of the need to prevent false news and to limit their spreading particularly during electoral periods has triggered initiatives ranging from research, education and cooperation to self-regulation and regulatory solutions, including at the international level. The NATO has set up a Stratcom Centre of Excellence, a think tank focusing on the impact of information domination on the internet and cyber defence. As a result of EU-NATO cooperation on hybrid threats, the European Centre of Excellence for Countering Hybrid Threats, was established in 2017.[93]

92. Several networks of people working together to fact-check online information exist, for example the International Fact-Checking Network (IFCN) works as a unit of the Poynter Institute that is dedicated to bringing together fact-checkers worldwide. The IFCN was created in 2015, to support and study the work of 64 fact-checking organisations from around the globe.

B. EUROPEAN UNION

93. In January 2018, the European Commission set up a high-level group of experts ("HLEG") to advise on policy initiatives to counter "fake news" and disinformation which is spread online. In its Final Report,[94] the HLEG recommended a multidimensional approach based on five pillars designed to:

    i) enhance transparency of online news;

    ii) promote media and information literacy to counter disinformation;

92. States may only impose restrictions on the right to freedom of expression in accordance with the test for such restrictions under international law, namely that they be provided for by law, serve one of the legitimate interests recognised under international law, and be necessary and proportionate to protect that interest.

93. See also the practical guide for the use of social media during elections which has been developed by the International Institute for Democracy and Electoral Assistance (International IDEA) for the benefit of electoral management bodies: Seema Shah, "Guidelines for the Development of a Social Media Code of Conduct for Elections", International IDEA, 2015.

    The guide is available at: www.idea.int/sites/default/files/publications/social-media-guide-for-electoral-management-bodies.pdf.

94. See ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-andonline-disinformation.

iii) develop tools for empowering users and journalists to tackle disinformation;

iv) safeguard the diversity and sustainability of the European news media ecosystem; and

v) promote continued research on the impact of disinformation in Europe.

94. Building on the output of the HLEG, the European Commission has issued in April 2018 a Communication outlining the Commission's strategy to tackle the problem of online disinformation.[95] Such strategy does not foresee a regulatory intervention and has as main lines of actions: i) the development of an ambitious self-regulatory Code of Practice by leading actors of the market (including social networks, advertisers and other players of the advertising industry); ii) the strengthening of fact checking and monitoring capacity on disinformation; iii) the use of new technologies (e.g. artificial intelligence) for tackling disinformation; iv) the reinforcement of the election processes; and v) the fostering of education and media literacy.

95. The Code of Practice on Disinformation has been adopted in September 2018[96] with the view of protecting the upcoming EU elections. The Code is aimed at:

- ensuring transparency about sponsored content, in particular political advertising, as well as restricting targeting options for political advertising and reducing revenues for purveyors of disinformation;
- providing greater clarity about the functioning of algorithms and enabling third-party verification;
- making it easier for users to discover and access different news sources representing alternative viewpoints;
- introducing measures to identify and close fake accounts and to tackle the issue of automatic bots;
- enabling fact-checkers, researchers and public authorities to continuously monitor online disinformation.

96. The European Commission, through the research and innovation Framework Programme Horizon 2020 has also supported several innovation actions to develop new tools and services to help professionals and citizens in verifying online content (text, image and video). Moreover, it will create an independent European network of fact-checkers, who will be selected from the European

95. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on "Tackling online disinformation: a European Approach", COM(2018) 236 final.
Available at: eur-lex.europa.eu/legalcontent/EN/TXT/HTML/?uri=CELEX:52018DC0236&from=EN.

96. Available at: ec.europa.eu/digital-single-market/en/news/code-practice-disinformation.

members of the IFCN. The network will develop working methods, establish best practices, in order to achieve the broadest coverage for factual corrections. The Commission will give the network the online tools needed, a secure European online platform on disinformation, to help it achieve its goal. Through the Connect Europe Facility (CEF), the Commission will also support the deployment of a European platform on disinformation to increase the capacity to detect and analyse disinformation campaigns across Europe.

97. In September 2018, the European Commission made specific recommendations with the aim to protect Europe's democratic processes from manipulation by third countries or private interests, and proposed new rules on election cooperation networks, online transparency, protection against cybersecurity incidents and steps to counter disinformation campaigns in the context of the European elections.[97] In December 2018, an Action Plan against disinformation[98] was adopted which is aimed at building up capabilities and strengthening cooperation between member states and EU institutions to proactively address the threats posed by disinformation. Attention is also drawn to the March 2018 Opinion by the European Data Protection Supervisor on online manipulation and personal data,[99] which recommends that data protection rules be completed and enforced, that regulators should aim for a collective diagnosis of the problem and cooperate across sectors, that self-regulation and codes of conduct be encouraged, and that individuals be empowered to exercise their rights including collective action.

98. Among already existing EU regulations, the following appear particularly relevant in the present context:

- The General Data Protection Regulation (GDPR)[100] which is directly applicable across the EU since 25 May 2018. Its provisions are mandatory and grant individuals numerous rights, including those to transparent communication, erasure (the right to be forgotten), and data portability (i.e. transfer from one data controller to another). The Regulation provides a general prohibition to process personal data "revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation" with some exceptions, notably when "processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall

97. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on "Securing free and fair European elections", COM(2018) 637 final. Available at: eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2018:637:FIN.
98. See ec.europa.eu/digital-single-market/en/news/europe-protects-eu-steps-action-against-disinformation.
99. Available at: edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf.
100. Available at: ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018reform-eu-data-protection-rules_en.

be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject". The rights established by the GDPR may be exercised and enforced not only by individuals but by organisations acting on behalf of individuals. To fill the protection gap from inadequate personal data processing outside of EU, the GDPR extends legal protection to the processing of personal data of EU data subjects "regardless of where the processing activities take place". This makes it applicable also to entities established outside the EU if they offer goods or services to individuals in the Union, or if they monitor their online behaviour. The regulation provides for strict rules on data transferring outside the Union; data processors must keep records of all processing activities. They are held responsible for adopting all necessary measures to guarantee that personal data is processed lawfully, fairly and in a transparent manner. The GDPR thus has the potential to prevent unauthorised personal data processing for electoral purposes, like in the case of Cambridge Analytica.[101]

- Regulation (EU) 2015/2120 laying down measures concerning open internet access,[102] applicable as of 30 April 2016, creates the individual and enforceable right for end-users in the EU to access and distribute internet content and services of their choice, and enshrines the principle of non-discriminatory traffic management. The enforcement of open internet rules within the EU is the task of national regulatory authorities which should respect the guidelines adopted by the body of European Regulators for Electronic Communications (BEREC) in 2016. Accordingly, it is not up to internet service providers to arbitrate the success or failure of the services and content distributed. The rules enshrine the principle of net neutrality into EU law and seek to prevent the blocking or throttling or discrimination of online content, applications and services.[103]

- Directive 2000/31/EC of the European Parliament and of the Council[104] contains liability exemptions available to certain online service providers including providers of "hosting" services, on the condition that they act expeditiously to remove or disable access to illegal information that they store ***upon obtaining actual knowledge thereof***. In this connection, it should be noted that the European Commission in several recent Communications stressed the need for online platforms to act more responsibly and step up EU-wide self-regulatory efforts to remove illegal content; on 1 March 2018, it adopted the Recommendation on measures to effectively tackle illegal online content[105] which is directed at member states and hosting

101. For information on the implementation of the GDPR in different European countries, see: www.gdprtoday.org/gdpr-loopholes-facilitate-data-exploitation-by-political-parties.
102. Available at: eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015R2120.
103. See ec.europa.eu/digital-single-market/en/open-internet-net-neutrality.
104. Available at: eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32000L0031.
105. Available at: ec.europa.eu/digital-single-market/en/news/commission-recommendationmeasureseffectively-tackle-illegal-content-online.

service providers, and which is aimed at enhancing transparency and the accuracy of notice-and-action mechanisms.

C. EXAMPLES AT THE NATIONAL LEVEL

99. Several States have recently adopted – or are planning to adopt – legislation to regulate online content and to counter politically loaded disinformation in their elections. Germany acted first[106] by obliging internet intermediaries (such as Facebook, Instagram, Twitter or YouTube) to promptly remove upon complaint any illegal content designated as such in the Criminal Code; obviously illegal content must be blocked or deleted within 24 hours. Offences range from hate speech and certain defamatory offences to content amounting to a threat to the constitutional order or national security, etc., which can have a direct impact on public debate and opinion especially during times of elections (the law is a general one, it is not specific to electoral campaigns). The Network Enforcement Act which took effect in the beginning of 2018 provides for fines up to € 50 million, which are applicable even if the offence was not committed in Germany.

100. In November 2018, the French Parliament adopted a law to combat manipulation of information[107] during electoral periods, which aims to identify and stop deliberate allegations of a false or misleading fact on an online platform in the three-month period before an election. Under the new legislation, platforms are subject to an obligation of transparency: they must give clear, correct and transparent information on their own identity and quality or of that of the third party for which it sponsors the content; they must also make public the amount received in exchange for sponsoring the content. A prosecutor, any person with legal interest in bringing the case before a judge on the basis of urgency, parties or candidates may complain about an item of allegedly false or implausible deliberately, artificially and massively disseminated information online; this notion of artificial and widespread dissemination will be a clue for false information. A judge is obliged to rule on a case of this nature within 48 hours, and has the right to block the publication and to force the platform to stop this campaign. Technical intermediaries, who are persons offering access to communication services, have to promptly remove any illicit content brought to their attention and implement an easily accessible and visible mechanism for persons to notify them of any false news. Moreover, the French Regulatory Broadcast Authority has the right to refuse to sign a convention with a foreign country if the latter's activities could seriously upset the life of the nation by the dissemination of false news or violated pluralism of streams of opinion.[108]

106. Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz – NetzDG) - Network Enforcement Act, germanlawarchive.iuscomp.org/?p=1245.

107. Loi n° 2018 1202 relative à la lutte contre la manipulation de l'information, www.legifrance.gouv.fr/affichTexte.do;jsessionid=EDB587F21F791D8941E5E11E82A0320A.tplgfr22s_1?cidTexte=JORFTEXT000037847559&categorieLien=id.

108. The French law has been the object of harsh criticism, see e.g. www.euronews.com/2018/11/22/francepasses-controversial-fake-news-law. In the case of Germany, see e.g. www.dw.com/en/germany-implements-new-internet-hate-speech-crackdown/a-41991590 and www.economist.com/europe/2018/01/13/germany-is-silencing-hate-speech-but-cannot-define-it.

101. Russia,[109] Singapore[110] and the Philippines have directly cited the German law as a positive example as they contemplate or have adopted legislation to remove "illegal" content online.[111]

102. The British Electoral Commission called on increasing transparency for voters with regard to the practice of digital electoral campaigns. It made recommendations about the responsibility of digital campaigns, spending on digital campaigns, transparency on payments for digital campaigns and enforcement of these rules.[112]

103. In the USA, the bipartisan Honest Ads Act presented in October 2017 before the US Congress[113] envisages disclosure and disclaimer rules to online political advertising. While television and radio have long been required to disclose the purchasers and content of all who purchase advertisements on their stations, internet companies have not. The Honest Ads Act would mandate that internet companies reveal the identities and content of advertisements related to elections or campaigns. Specifically, this would be done by amending a decades-old existing campaign finance law from 1971, by adding the phrase "paid internet or paid digital communication" to its list of media forms subject to the law. It would also require any website with at least 50 million monthly viewers - including Facebook, Google, and Twitter - to maintain a public list of any organisation or person who spends at least $500 in election-related advertisements. An exemption is made for "news story, commentary, or editorial" to ensure that the requirements are not levied on legitimate news reporting or opinion pieces.

104. In some countries, specialised units to combat information disorder have been or are being created, for example:

- a) In the United Kingdom it is planned to set up a national security communications unit to tackle "fake news" disinformation.

109. Federal Law "On information, information technologies, and protection of information" (of 27 July 2006, no. 149-FZ) was adopted on 18 March 2019. It penalises the spread of "unreliable socially important information" that could endanger lives and public health, raise the threat of massive violation of public security etc. This law permits to block the web-page containing such information. On the same day Federal Law no. 30-FZ (the "disrespect law") was adopted, adding Article 15-1-1 to the Federal Law "On information, information technologies, and protection of information" (of 27 July 2006, no. 149-FZ). It penalizes expression which "shows disrespect towards the society, the State, official State symbols … and organs of State power" and which is expressed in "obscene form". The Code of Administrative Offences was amended to introduce fines for publications containing "obscene disrespect" and "fake news".

110. techcrunch.com/2019/05/09/singapore-fakenewslaw/?renderMode=ie11&guccounter=1&guce_referrer_us=aHR0cHM6Ly90ZWNoY3J1bmNoLmNvbS8yMDE5LzA1LzA5L3NpbmdhcG9yZS1mYWtlLW5ld3MtbGF3Lw&guce_referrer_cs=oKT9smcHtaNhdWGcU8VGvg; mediawrites.law/fake-news-law-passed-in-singapore-protection-from-online-falsehoods-and-manipulationact.

111. See www.hrw.org/news/2018/02/14/germany-flawed-social-media-law.

112. See www.electoralcommission.org.uk/__data/assets/pdf_file/0010/244594/Digital- campaigningimproving-transparency-for-voters.pdf.

113. www.congress.gov/search?q=%7B%22source%22%3A%22legislation%22%2C%22search%22%3A%22Honest%20Ads%20act%22%7D&searchResultViewType=expanded.

- b) In the Czech Republic, the Centre Against Terrorism and Hybrid Threats, part of the Interior Ministry, it is a specialised analytical and communications unit that monitors threats directly related to internal security, which implies a broad array of threats and potential incidents relative to terrorism, soft target attacks, security aspects of migration, extremism, public gatherings, violation of public order and different crimes, but also disinformation campaigns related to internal security. It also develops proposals for substantive and legislative solutions that it also implements where possible and disseminates information and spread awareness about the given issues among the general and professional public.

105. Cooperation among electoral authorities, academics and practitioners has been fostered in Brazil in order to assess the true impact and efficiency of adopted measures, through the Advisory Council for Internet and Elections that advises the Electoral Tribunal. Panama and Mexico[114] are examples of countries where operators and platforms have been cooperating with electoral authorities in order to detect threats and to spread official information.

106. Fact-checking[115] has been developing in many countries[116] and in some of them, networks of fact-checkers have been set up; an interesting example is "#Verificado2018", a group of journalists, civil society and academic partners that sought to debunk viral misinformation, fact check politicians' claims and combat fake news for the 2018 electoral federal process in Mexico. Spain also established a special fact-checking unit during the last elections.[117]

VII. E-CHALLENGES TO DEMOCRACY AND HUMAN RIGHTS

107. The holding of democratic elections, hence the very existence of democracy are impossible without respect for human rights, particularly the freedom of expression and of the press and the freedom of assembly and association for political purposes, including the creation of political parties. Respect of these freedoms is vital particularly during election campaigns. Restrictions on these fundamental rights must comply with the European Convention on Human Rights and, more generally, with the requirement that they have a basis in law, are in the general interest and respect the principle of proportionality. Clear criteria for balancing the competing rights should be set out in the legislation and effectively implemented through electoral and ordinary justice mechanisms.

114. INE (Instituto Nacional Electoral) of Mexico, during the preparation of the 2018 elections, entered into cooperation agreements with Facebook, Twitter and Google; see INE, Democracia en riesgo, Elecciones en tiempos de desinformación, Estrategia y acciones implementadas para enfrentar la desinformación deliberada en las elecciones mexicanas de 2018.

115. Cf. Lazer et al., 2018.

116. See e.g. the Appendix of the CoE Information Disorder Report 2017 which lists European fact-checking and debunking initiatives. See also reporterslab.org/fact-checking.

117. elpais.com/politica/2019/03/10/actualidad/1552243571_703630.

108. Several specific notions of democracy are affected by the use of digital technologies. First, new information technologies - the electronic vote and the formation and actualisation of centralised registers of voters for example - make an impact on ***electoral democracy***, understood as the institutional activities and infrastructure that make elections possible, and commonly known in the internet context as "e-government". Second, the internet and new information technologies have the potential to allow for greater transparency and accountability, as well as for broader and more efficient forms of political participation, extending the reach of the "public sphere"; in this sense, they impact on ***deliberative democracy***, which refers to participation by individuals in open debate in the belief that it will lead to better decisions on matters of common concern.[118] Finally, to the extent that these technologies facilitate a process whereby large disorganised groups of people organise and act to address specific social, economic or political issues, they may be seen as having an influence on the so-called ***"monitory democracy"***, defined as "the public accountability and public control of decision makers, whether they operate in the field of state or interstate institutions or within so-called non-governmental or civil society organisations, such as businesses, trade unions, sports associations and charities".[119] To the extent that the citizens' capacity to survey and selforganise for political purposes depends both on the information they can access and on their possibilities to deliberate and agree on a common agenda, the monitory democracy variables may be considered as embedded in the deliberative democracy category.

A. CHALLENGES TO ELECTORAL DEMOCRACY

109. As mentioned earlier, the concept ***"electoral democracy"*** refers to the institutional activities and infrastructure that make elections possible. From the organisation of the election itself, to the creation and administration of voters' registers or the implementation of electronic ballots and internet voting, the electoral aspect of democracy sets the material and institutional conditions necessary to translate the popular suffrage into the appointment of representatives or the approval of laws and public policies. The proper maintenance of electoral registers, for example, is crucial to the realization of the principle of universal suffrage; the strict observance of the voting and counting procedures is crucial to the realization of the principle of free suffrage.

110. If on the one hand the use of digital technologies may make democratic processes more accessible to all citizens, it may also bring about obstacles to the exercise and development of electoral democracy, entailing new forms of undue interference with the right to vote and the right to stand for election

118. Laidlaw 2015, p. 10-11.

119. John Keane, The Life and Death of Democracy,2009. The definition of "monitory democracy" is given at thelifeanddeathofdemocracy.org/glossary/monitorydemocracy.

(Article 3 of Protocol 1 ECHR), the right to freedom of expression (Article 10 ECHR) and the right to respect for private life (Article 8 ECHR).

111. According to the Communications Security Establishment (CSE) of the Government of Canada, "[a]dversaries worldwide use cyber capabilities… against elections… to suppress voter turnout, tamper with election results, and steal voter information… against political parties and politicians... to conduct cyberespionage for the purposes of coercion and manipulation, and to publicly discredit individuals… [and] against both traditional and social media… to spread disinformation and propaganda, and to shape the opinions of voters".[120] Furthermore, the CSE estimates that "it is highly probable that cyber threat activity against democratic processes worldwide will increase in quantity and sophistication" over the next years for the following reasons:[121]

- *Many effective cyber capabilities are publicly available, cheap, and easy to use.*
- *The rapid growth of social media, along with the decline in longstanding authoritative sources of information, makes it easier for adversaries to use cyber capabilities and other methods to inject disinformation and propaganda into the media and influence voters.*
- *Election agencies are, increasingly, using the internet to improve services for voters. As these services move online, they become more vulnerable to cyber threats.*

120. CSE 2017. We have seen several examples of these interventions around the world:
    - "In June 2016, the US state of Arizona shut down its voter registration system for nearly a week after adversaries attempted to gain access to the system. The next month, in Illinois, the state election agency took down its website for two weeks after discovering tens of thousands of voter records (e.g. names, addresses, and driver's licence numbers) were suspected to have been viewed by the adversaries" (Nakashima, as referred by the CSE).
    - "Responding to perceived software vulnerabilities in its vote tabulation machines and warnings that the election may be targeted by Russia, the Netherlands amended voting procedures in their most recent election. To avoid the possibility of adversaries interfering with the election, all votes were hand-counted" (Escritt, as referred by the CSE).
    - "In December 2016, adversaries gained access to the website of Ghana's Central Election Commission during the general election as the votes were being counted. An unknown adversary tweeted fake results that the incumbent candidate had lost. The electoral commission then sent out its own tweets claiming these results to be false. While the outcome of the election was not altered, this incident served to sow confusion in the minds of many voters" (BBC News, as referred by the CSE).

      "In the last US presidential election, both major political parties were subjected to cyberespionage attempts by Russia. Russian operatives used cyber capabilities to gain access to the emails of key political staff working on the Democratic Party campaign. The emails were subsequently leaked to embarrass the Democratic Party candidate" (ODNI, as referred by the CSE).
    - "According to media reports, French intelligence believes that social botnets were used to influence the presidential election. Certain social media accounts, the same ones that were active during last year's US election, were promoting false and defamatory information against a leading candidate. In the final days of the election, one party was also victimised by the unauthorised release of thousands of campaign-related emails" (Auchard, as referred by the CSE).
    - "Cyberwarfare, once a largely hypothetical threat, has become a well-documented reality, and attacks by foreign states are now a credible threat to a national online voting system. As recently as May 2014, attackers linked to Russia targeted election infrastructure in Ukraine and briefly delayed vote counting" (Springall et al. 2014).
121. CSE 2017.

- *Deterring cyber threat activity is challenging because it is often difficult to detect, attribute, and respond to in a timely manner. As a result, the cost/benefit equation tends to favour those who use cyber capabilities rather than those who defend against their use.*

- *Finally, there is a dynamic of success emboldening adversaries to repeat their activity, and to inspire "copycat behaviour".*

112. The Council of Europe Convention on Cybercrime ETS 185 of 2001 ("Budapest Convention") and the current work on a 2nd Additional Protocol to this treaty show that many states have understood the risks.[122]

113. From a cybercrime perspective, threats to electoral democracy may involve at least two types of interference. One type is attacks against the confidentiality, integrity and availability of election computers and data, including:

- compromising voter databases or registration systems, for example, through hacking of computer systems or deleting, altering or adding data;
- tampering with voting machines to manipulate results;
- interfering with the functioning of systems (for example, a distributed denial of service attack on election day);
- illegally accessing computers to steal, modify or disseminate sensitive data such as, for example, the theft of data from election campaign computers for use in information operations.

114. Such attacks clearly represent forms of cybercrime as defined in the Budapest Convention on Cybercrime, such as illegal access to computer systems (Article 2), illegal interception (Article 3), data and system interference (Articles 4 and 5) and others. The currently more than sixty Parties to this treaty have transposed these provisions into their domestic law.

115. As mentioned earlier, these attacks amount to an interference with several fundamental rights guaranteed by the ECHR and other international human rights instruments. They may be carried out by governments, political parties/candidates, foreign powers and private actors. In this respect, it needs to be stressed that under the ECHR states have a positive obligation to ensure free and secure elections and to guarantee human rights such as the right to private life and the freedom of expression.

116. A second type of attack involves (dis-)information operations – which do not constitute cybercrime but violate the rules on the protection of personal data, on political finances, on media coverage or on the broadcasting of elections,

122. "Cybercrime in the election process: the role of the Budapest Convention", www.venice.coe.int/files/15EMB/Alexander_Seger.pptx

that is, rules to ensure free, fair and clean elections. The evidence that such rules are broken often takes the form of electronic evidence, that is, it is evidence found on computer systems. It is essential, therefore, that states provide their criminal justice authorities with the necessary powers to secure such evidence. Parties to the Budapest Convention are required to do so under Articles 16 to 21.

117. International standards indeed point to a responsibility of the States to prevent inequality in media coverage of electoral campaigns and to ensure that citizens are informed on political parties in order to make an informed free political choice of their representatives. In addition to their obligations not to unduly interfere with the enjoyment of fundamental rights, States also have positive obligations to prevent that violations be committed by third parties. A fair balance needs to be provided by conflicting rights. The undue use of the voters' registry data for electoral purposes or the excessive disclosure of a candidate's personal information in the heat of a political campaign are common scenarios of such conflicts. Most democracies would deem the first scenario as a clear violation of the right to privacy and a breach to electoral equity, even if political parties have the right to access such information. It may be argued however that the nature of the democratic debate would allow for an extended permissiveness of the political right of expression over the candidate's right to privacy, provided that those expressions do not clearly constitute defamation or slander. Contemporary democracies are used to these scenarios and have produced a rather abundant set of rulings and national legislation on the matter.

118. For at least two decades, several countries have experimented with internet voting to strengthen political rights. For instance, in the year 2000, Switzerland launched the project "vote électronique" to test its reliability. Since then, the country has conducted more than 150 trials at the federal level and some cantons have made e-voting available for their citizens. In 2008, Norway also started testing internet voting and made some trials during the 2011 municipal elections and the 2013 parliamentary elections. In Canada, internet voting is available in some provinces (Ontario and Nova Scotia) since 2003. Perhaps the most successful experiment has been carried out by Estonia, where discussions about internet voting began in 2001 and since 2005 it has been considered as an additional and legally binding form of voting.[123]

119. Notwithstanding the success of some trials, the use of the internet for casting votes has raised several security concerns. "Estonia was the first country in the world to use internet voting nationally, and today more than 30% of its ballots are cast online", but researchers from the University of Michigan and the Open Rights Group have found "that the [Estonian] I-voting system has serious architectural limitations and procedural gaps that potentially jeopardise the integrity of elections" to the extent that

123. ACE Project 2018.

"attackers could target the election servers or voters' clients to alter election results or undermine the legitimacy of the system." Their concerns were such that they concluded that "[s]omeday, if there are fundamental advances in computer security, the risk profile may be more favorable for internet voting, but we do not believe that the I-voting system can be made safe today".[124]

120. In this context, it should be stressed that it may be that misinformation and blanket digital interference with political discourse is aimed not a subverting the mechanics of the election itself but rather at undermining public trust in the process and public trust in the political system. The openness of a liberal democracy is a strength but also a vulnerability. Digital technologies should not be allowed to sap the confidence of the public in the electoral process, hence the necessity of reassuring the public about the security of such technologies. To this end, digital technologies should be introduced gradually and may be combined with traditional methods. Innovation cannot come at the cost of legal requirements, including security.

121. These challenges need to be addressed from an interdependent stance, which means to that (1) the transnational nature of the problem and (2) the essential role played by the gatekeepers of information highways (i.e. internet service providers) to investigate and prosecute cybercrimes must be recognized. The international framework needs to be strengthened in order to establish more efficient mechanisms of transnational cooperation among nations and private actors, and, if possible, to procure a greater uniformity among national legislations. In the end, the solution seems to be "to adapt the constitutional framework of modern democracies" to the new electronic environment in which cybercrime thrives and in which governments, corporations and citizens interact and make democracies possible.[125]

B. CHALLENGES TO DELIBERATIVE DEMOCRACY

122. The principle of free suffrage is grounded on the freedom of voters to form an opinion. This freedom, which partly overlaps with equality of electoral opportunity, requires the state, and public authorities generally, to honour their duty of even-handedness, particularly where the use of the mass media, billposting, the right to demonstrate on public thoroughfares and the funding of parties and candidates are concerned.[126] The freedom to form an opinion includes the right to be correctly informed before making a decision, the right to private online browsing and the right to make confidential communications on the internet. The monitoring of people's online activity without their consent and for the purpose of understanding and exploiting their behavioral paths undermines these rights.

124. Springall et al. 2014.

125. Mecinas Montiel 2016, p. 427.

126. Venice Commission, Code of good practice in electoral matters, explanatory report, Free suffrage.

123. Technology is changing the way electoral campaigns are managed. The internet is a powerful platform for political parties to present their agenda to the electorate and to mobilise a larger support base for their causes. The cost of communicating with voters can be substantially lower via this medium than via broadcast media, given the availability of free blog and video sharing platforms and social media. Small political parties with limited resources and independent candidates in particular can benefit from this type of communication.

124. However, the changes in the production and consumption of election-related content pose challenges for established institutions and principles of regulation of election communications such as freedom of association, spending limits and regulation of political advertising. They undermine the ability of existing regulation to maintain the level playing field in electoral communication between new and established, rich and poor, corporate and civil society campaigns. New intermediaries and platforms now occupy the important gatekeeper positions once occupied by journalists, but have not yet adopted the ethical obligations of the media. This presents a threat to elections and potential for corrupt practices to emerge. The CoE Election Study 2017 identifies a number of concerns for the fairness and legitimacy of electoral processes, such as the lack of transparency of campaigning, spending, messages and algorithms used in digital advertising, large-scale invasions of privacy, lack of journalism filter to fact-check political messages, the increased amount of disinformation, and lacunas in electoral campaigning regulation (e.g. impossibility to enforce silence periods), and which concludes that "the current regulatory framework no longer suffices for maintaining a level playing field for political contest and for limiting the role of money in elections."[127]

125. Traditional electoral campaigning is being challenged by new forms of communication channels which are not only a help in spreading a message at a low cost but also make use of specific marketing techniques that best adapt to specific sections of the electorate. Mechanisms such as the use of personalized ads and messages, which are applicable to any field of digital marketing, have been recently used in the electoral arena providing some actors who have access to these mechanisms with a non-transparent advantage. Electoral messages have thus become increasingly personalized. Those who design campaigns do not have to think about the majority of the electorate who have already their mind set on how to cast their vote. As such, they can concentrate on small groups of swing voters. The new campaign techniques provide with the possibility of tailored electoral messages

127. CoE 2017 Election Study; See also the 2018 report on "Disinformation and electoral campaigns" (Doublet, 2018, CDDG(2018)11), which suggests the preparation by the Council of Europe of a broad Programme of Action in this area. It recommended, for example, defining the length of electoral campaigns to avoid the risk of significant digital campaigns before the electoral campaign period; requiring imprints of digital material to know who is behind online platforms; obtaining disclosure of spending made on digital electoral campaign activity by online platforms; banning funding of digital electoral expenditure by a foreign physical or legal person.

somewhat disguised as general, politically neutral messages. Exercising such hidden influence is facilitated by the use of social platforms, not only because of their data processing algorithms but mainly because they provide with the possibility of directly targeting specific groups of profiles with personalized ads and messages, while the targeted users do not detect the personalisation. With the aid of technology, campaigning techniques have shifted to an evolutionary concept of the one to one or the many to many approach: this is what Joseph Pine calls "mass customization".[128] Unlike the traditional mass media, which in principle have a declared political colour which is known to the reader, internet providers do not have a declared political line, so that in the absence of a clear indication that the information provided by them is in fact a partisan political ad, the users may be under the impression that such information is politically neutral.

126. The manipulation of electoral preferences has been examined by Rob Epstein, and more particularly the influence of search engines rankings (especially Google for its predominance) on voting preferences (referred to as Search Engine Manipulation Effect, SEME).[129] According to a 2015 study, higher-ranked items connected with web pages that favor one candidate, have an impact on the opinions of undecided voters.[130] Evidence from five experiments in two countries suggests that "(i) biased search rankings can shift the voting preferences of undecided voters by 20% or more, (ii) the shift can be much higher in some demographic groups, and (iii) such rankings can be masked so that people show no awareness of the manipulation." The authors of the study conclude that "if Google favours one candidate in an election, its impact on undecided voters could easily decide the election's outcome." While the results of this study may need to be corroborated by further research, one might concur with the authors' conclusion that it is "even more disturbing" that "the search-ranking business is entirely unregulated".

127. In this context, it should be borne in mind that search engine rankings are a product of complex algorithms and are not necessarily manipulative in design, but are in fact aiming to provide the most topical, relevant and new results; however, the algorithms can be manipulated by different websites trying to acquire better rankings. In reality, we see that happening, and Google is constantly improving the search algorithm to prevent such intrusions. In any case, whether manipulation is intentional or not, the SEME entails two important consequences for democracy: the power to manipulate preferences could be used by private or public actors to affect electoral equity; and the fact that search-engine users are unaware of the criteria (coding) of the ranking mechanisms hinders their capacity to make fully informed decisions, and therefore to exert their freedom of expression.

128. PINE, B.J., II. (1993). Mass Customization: The New Frontier in Business Competition. Harvard Business School Press, Boston.

129. Epstein 2016.

130. Epstein and Robertson 2015.

128. The SEME is not exclusive of online search engines. Social media platforms are also governed by an underlying coding architecture that is not unbiased. Companies like Facebook, Twitter or Instagram, unlike the traditional media, are not politically oriented; they are primarily motivated by commercial interests and design their coding structure according to those interests. In this sense, the algorithms that govern social media foster a partial and sometimes illusory comprehension of politics and democracy, because they provide biased information that reflect the partial interests and behaviour of their users.[131]

129. Indeed, social media and search-engine companies can shape online social interactions not only because they have the power of coding the environments of such interactions, but also because of their capacity to profile ("profiling") and predict their user's attributes and behaviours. These companies can easily access "digital records of behaviour, such as Facebook Likes, browsing histories, search queries, or purchase histories can be used to automatically and accurately predict a range of highly sensitive personal attributes including: sexual orientation, ethnicity, religious and political views, personality traits, intelligence, happiness, use of addictive substances, parental separation, age, and gender".[132] Furthermore, these architects can process such information to create highly accurate profiles of their users, predict their preferences, and even target them with individualised data and advertising in order to promote or discourage specific behaviours.[133]

130. On one side, companies like Facebook or Google commoditise their users' information and sell them in the market. Buyers, on the other side, use such information with little or no accountability to influence consumers and sometimes voters, through "tailored ads based on personal data".[134] That was exactly the case of Cambridge Analytica. The current business model for many websites offers content in exchange for personal data. The fact that people give away their personal information in exchange for free services enables widespread data collection by the websites which may lead to their use and misuse by various actors.

131. Even if it is true that social media users must explicitly accept the general privacy conditions imposed by the social media companies, they have little

131. Van Dijck 2013; McChesney 2013.

132. Graepel et al. 2013.

133. For instance, according to an account by Robert Epstein (2016):

"… a study by Robert M Bond, now a political science professor at Ohio State University and others, published in Nature in 2012, described an ethically questionable experiment in which, on election day in 2010, Facebook sent 'go out and vote' reminders to more than 60 million of its users. The reminders caused about 340,000 people to vote who otherwise would not have. Writing in the New Republic in 2014, Jonathan Zittrain, professor of international law at Harvard University, pointed out that, given the massive amount of information it has collected about its users, Facebook could easily send such messages only to people who support one particular party or candidate, and that doing so could easily flip a close election – with no one knowing that this has occurred. And because advertisements, like search rankings, are ephemeral, manipulating an election in this way would leave no paper trail."

134. Christopher Wylie, as quoted by Guimón 2018.

or no control on who is authorised to "buy" their personal information, or to what uses it should be put. This situation undermines the fundamental right to privacy and personal data protection, because it curbs the user's capacity to impose limits on the use of his/her personal information.[135] In the ruling 292/2000, the Constitutional Tribunal of Spain established that "the fundamental right to the protection of personal data… grants the incumbent with a set of powers to impose on third parties the duty to perform or refrain from performing specific behaviours, which grants the individuals with the power to decide over their data… [a useless power] if the incumbent has no knowledge of what information is in the hands of third parties, who are those parties, and to which use will the information be put."[136]

132. The use and abuse of personal data for electoral purposes, cloaked as freedom of commerce, might pose a serious threat to free elections and electoral equity at least in three aspects: first, because private actors might use such information to directly exert undue influence on the electoral competition; second, because internet and social media companies, arguing freedom of commerce, might restrict the access to such information according to their political preferences, hence granting an opaque advantage to some parties or candidates over others; and third, because the commoditisation of personal data represents a challenge to the surveillance of money in political campaigns.

133. The risk to undermine the rights to privacy, free elections/electoral equity and freedom of expression and opinion – and, as some experts argue, even freedom of thought – suggests a need to regulate the commercial rights of internet and social media companies. That said, to completely forbid the "commoditisation of information" would also hinder the development of the internet and, consequently, the access to an apparently limitless source of political information and democratic action. As long as societies do not find new forms to finance the internet, to impose excessive limits on the commoditisation of personal information could curtail fundamental political rights such as freedom of expression and freedom to organise political action. The paradox is that the same technologies that have enhanced the possibilities of expression, are the ones that curtail such possibilities.[137]

134. On the one hand, the right to access the internet is a necessary condition for the full exercise of freedom of expression, which is a necessary condition for

135. Davara 2003, p. 43-44.

136. As referred by Davara 2003. Own translation.

137. In the words of Laidlaw (2015, p. xi-xii):*"[T]he communication technologies that enable or disable participation in discourse online are privately owned…Thus, we inevitably rely on these companies to exercise the right to freedom of expression online, and they thereby become gatekeepers to our online experience… Our reliance on these gatekeepers to exercise the right to free speech has had two effects. First, such gatekeepers have increasingly been the target of legal measures designed to capitalise on their capacity to regulate third-party conduct… Second, …speech regulation in cyberspace has largely been left to self-regulation, in much the same way that regulation of the internet in general has been light-touch…. The result is a system of private governance running alongside the law, without any of the human rights safeguards one normally expects of state-run systems, such as principles of accountability, predictability, accessibility, transparency and proportionality".*

the existence of a democratic society.[138] On the other hand, the internet itself poses different sets of threats to democracy. As social media and the internet are not (and should not be) a space located outside legal parameters,[139] there is an urgent need to find solutions to these conflicts of rights that allow for a reasonable protection of privacy, political and commercial rights.

135. The lack of or insufficient regulation of the Internet and social media has left users with no legal recourse to protect their data and, most of all, their freedom of expression and democratic rights. On the one hand it is problematic when private technology companies are censoring content which they consider "harmful", without them being accountable and their measures being transparent.

136. On the other hand, the positive responsibility of the state to prevent undue interference by third parties must not lead to undue state intervention, through excessive or undue regulation which can result in undermining the very rights that it is meant to protect. Unjustified state surveillance of private communications and the different ways in which online platforms may be used so as to – intentionally or accidentally – affect the flow of information, directly curb the freedom of expression, hinder democratic dialogue, and infringe the principles of institutional neutrality and electoral equity. While it is understandable, in the context described above, that currently many states have on their agenda to tackle the issue of "fake news" with legislation, this may pose a threat to the fundamental right of freedom of expression and information – bearing in mind that exaggerated speech enjoys protection under international human rights standards such as Article 10 ECHR. Enabling the authorities to interfere with the public discourse may be abused to silence dissidents and prevent discussion which challenges mainstream thought and restricting criticism of societal attitudes. As the Venice Commission emphasised, "the mass media are not the only category that should be entitled to a high level of freedom of expression. Thus, persons who impart information and ideas on matters of public interest and contribute to the public debate on such matters, including members of campaign groups and elected

138. Lingens v. Austria, Application no. 9815/82 (ECtHR, 8 July 1986): "freedom of expression, as secured in paragraph 1 of Article 10 (art. 10-1), constitutes one of the essential foundations of a democratic society". Furthermore, in the case of Ahmet Yıldırım v. Turkey (Application no. 3111/10, 18 December 2012), the ECtHR has ruled that internet blocking may be "in direct conflict with the actual wording of paragraph 1 of Article 10 of the Convention, according to which the rights set forth in that Article are secured "regardless of frontiers"". See also Laidlaw (2015, p. 19-21):

"Democracy has always been embodied in the practices of communication, and freedom of expression has consistently been identified by the courts as central to democracy. In Lingens v. Austria, the European Court of Human Rights (ECtHR) famously commented that freedom of expression "is one of the essential foundations of a democratic society"…

Many states, such as Estonia, Finland, France, Greece and Spain, have legislatively recognised internet access as a fundamental right. In 2003, the Committee of Ministers of the Council of Europe adopted a Declaration affirming the importance of freedom of expression on the internet. Since 2010, we have seen a paradigm shift at an international level in the recognition of human rights in the cyberspace. Access to the internet as a fundamental right received the United Nations (UN) stamp of approval in a report by Frank La Rue, the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression… This was followed up in 2012 by the UN Human Rights Council passing a resolution affirming internet freedom as a basic human right, in particular the right to freedom of expression".

139. Electoral Tribunal of Mexico, g.

representatives, should be allowed a high level of freedom of expression, including a certain degree of exaggeration and even provocation as long as they act in good faith and exercise due diligence in order to provide accurate and reliable information".[140]

137. The filtering, blocking and take-down of illegal content on the internet in order to combat notably hate crimes and national security, as well as to protect intellectual property and privacy or defamation rights are a necessary but delicate exercise which however may be abused and result in censorship and in illegitimate silencing of political opponents. Any such measures must be in accordance with the law, which includes a precise and narrow definition of the offences in cause,[141] and it must pursue one of the legitimate aims listed in Article 10 ECHR. The criteria of necessity in a democratic society and proportionality must always be respected.[142] Effective judicial review by independent and impartial courts must be guaranteed.

138. As regards "fake news", most of which do not fall under any of the categories that would allow prosecution, alternative means need to be employed, such as fact-checking (which, while not a panacea, is becoming more advanced and effective), media literacy programmes aimed at sensitisation about the problem and recognition of false content, and investments in quality journalism.[143] In this endeavour, state authorities will need the cooperation of both citizenry and internet corporations.

139. At the same time, it must be stressed that any measures to address the information disorder must be designed with great care, so as not to undermine the "net neutrality". This is the founding principle of the internet, whereby ISPs are to treat all online data equally and provide the conditions for unfettered user access, without discrimination based on content or source. Protecting the democratic function of the internet from being monopolised by private corporate power calls for the equal treatment of all data sent and received without differential charges and service quality.[144] Abolishing the policy of "net neutrality", as the United States Federal Communication Commission agreed to do in December 2017,[145] allows ISPs to block or

140. CDL-AD(2013)024, Opinion on the legislation pertaining to the protection against defamation of the Republic of Azerbaijan, para. 37.

141. See for example Venice Commission, Opinion the Federal law on combating extremist activity of the Russian Federation, CDL-AD(2012)016.

142. See for example Venice Commission, Opinion on law no. 5651 on regulation of publications on the internet and combating crimes committed by means of such publication ("the internet law") of Turkey, CDL-AD-2016)011.

143. Cf. the CoE Information Disorder Report 2017 which offers more than 30 recommendations for different stakeholders.

144. From the perspective of both constitutional law and international human rights law it is crucial to take into account the reality of the influential actors outside the elected authorities preventing the realisation of fundamental rights. See Thorgeirsdóttir, Herdis (2005), Journalism Worthy of the Name: the Affirmative Side of Article 10 of the ECHR, Kluwer Law International.

145. The net neutrality regulations enacted in 2015, which sought to stop the ISPs giving preferential treatment to sites and services that paid them to accelerate their data, officially expired in June 2018.

throttle (slow down) websites and charge for faster download and upload speeds. In such circumstances, online services, applications, and websites can be granted preferential treatment for any number of reasons, be they commercial or ideological – including in less democratic countries where ISPs are state-owned and censored, and where authorities may be tempted to give faster lanes of access to pro-government outlets.

140. To conclude, while excessive or inadequate regulation of the internet might be counterproductive and hinder the accessibility and development of the internet and, consequently, the freedom of expression and the democratic dialogue itself, the problem of disinformation disorder cannot be left unattended. The risk to undermine the rights to privacy by the misuse of personal information, and the damages to freedom of expression and electoral equity produced by the architecture of the internet (i.e. SEME, epistemic bubbles, echo chambers and fake news), along with the lack of regulation which has left citizens with no efficient legal recourse to protect their personal and political rights, are situations that call for urgent action.

141. Such action must include the powerful private actors who, while motivated by primarily commercial interests, have the power to hamper human rights, while maintaining an essential platform for democracy, and must recognise such responsibility.

VIII. CONCLUSIONS

142. The holding of democratic elections, hence the very existence of democracy, is impossible without respect for human rights, particularly the freedom of expression and of the press and the freedom of assembly and association for political purposes, including the creation of political parties. Respect of these freedoms is vital particularly during election campaigns. Restrictions on these fundamental rights must comply with the European Convention on Human Rights and, more generally, with the requirement that they have a basis in law, are in the general interest and respect the principle of proportionality. Clear criteria for balancing the competing rights should be set out in the legislation and effectively implemented through electoral and ordinary justice mechanisms.

143. The relationship between democracy and digital technologies is quite complex. On the one hand, the internet and social media have become the dominant platform of political interaction in some democracies, the use of those tools have strengthened the critical attitudes of citizens towards their governments and their widespread use facilitates the organisation of large-scale social movements and a closer interaction between citizens and political parties. On the other hand, the new virtual tools may be used, and sometimes are indeed used against elections to suppress voter turnout, tamper with election results, and steal voter information; against political parties and politicians to conduct cyber espionage for the purposes of

coercion and manipulation, and to publicly discredit individuals; and against both traditional and social media to spread disinformation and propaganda, and to shape the opinions of voters. The new digital realm allows for new forms of criminality and data commercialisation that seriously threaten privacy rights, and modulates social interactions by selectively (and sometimes strategically) feeding or hiding specific information to its users, thus fostering a partial understanding of reality and hampering freedom of expression.

144. The internet-based services have enriched and diversified news sources, facilitating individuals' access to information and their decisions on the most crucial matters in democracy, notably on the choice of their legislature. However, at the same time, information disorder – misinformation, disinformation and malinformation – may distort the communication ecosystem to the point where voters may be seriously encumbered in their decisions by misleading, manipulative and false information designed to influence their votes. This environment potentially undermines the exercise of the right to free elections and creates considerable risks to the functioning of a democratic system.

145. The small number of very powerful private actors that literally own the information highways have own commercial interests and rights that tend to collide with both civil and political rights and electoral principles. These internet providers have taken up the gatekeeping role which originally belonged to the traditional media, without however having adopted the ethical obligations of the media. Private technology companies are thus censoring content which they consider "harmful", without them being accountable and their measures being transparent. It is true that social platforms have recently adopted a series of measures for preventing false news and limiting their spread particularly during electoral periods. There is a concept of corporate social responsibility, some sort of self-regulation for businesses with the primary goal of "doing no harm" and abiding by the rule of law and human rights principles, including the right to a remedy for their users, and being liable for their products (under commercial law, competition law, environmental law, etc.).[146] However, this is done on a voluntary and unregulated basis, without a recognised rule of law based framework.

146. While states have a positive responsibility to prevent undue interference with civil and political rights by third parties, undue state intervention through excessive or undue regulation can result in undermining the very rights that it is meant to protect. Unjustified state surveillance of private communications and the different ways in which online platforms may be used so as to – intentionally or accidentally – affect the flow of information, directly curb the freedom of expression, hinder democratic dialogue, and

146. Facebook, Google and Twitter are signatories to the Code of Practice against disinformation and have committed to report monthly on measures taken ahead of the European Parliament elections in May 2019: see the April reports on the implementation of the Code of Practice, ec.europa.eu/digital-single-market/news-redirect/651264.

infringe the principles of institutional neutrality and electoral equity. Enabling the authorities to interfere with the public discourse may be abused to silence dissidents and prevent discussion which challenges mainstream thought and restricts criticism of societal attitudes. In particular, the filtering, blocking and take-down of illegal content on the internet in order to combat notably hate crimes and to protect national security, as well as intellectual property and privacy or defamation rights must be in accordance with the law, which includes a precise and narrow definition of the offences in cause, and it must pursue one of the legitimate aims listed in Article 10 ECHR. The criteria of necessity in a democratic society and proportionality must always be respected. Effective judicial review by independent and impartial courts must be guaranteed.

147. As regards "fake news", alternative means need to be employed, such as factchecking, media literacy programmes aimed at sensitisation about the problem and recognition of false content, and investments in quality journalism.

148. At the same time, it must be stressed that any measures to address the information disorder must be designed with great care, so as not to undermine the principle of "net neutrality". The internet should remain an open platform.

149. To face these challenges, several measures need to be ensured from an interdependent and global perspective, notably:
As regards electoral democracy:

- A. Criminalise cyber-attacks against the confidentiality, integrity and availability of election computers and data in pursuance of the Budapest Convention on Cybercrime:

- B. Provide the criminal justice authorities with the necessary powers to secure electronic evidence of violations of rules on protection of personal data, on political finances, on media coverage or on the broadcasting of election;

- C. Prepare national Electoral Management Bodies (EMBs) for emergency situations and have in place crisis management organization; EMBs should be provided with adequate resources and training to adopt digital technologies and address the related cybersecurity risks;
As regards deliberative democracy:

- D. Recognise (1) the transnational nature of the problem and (2) the essential role played by the internet intermediaries (i.e. internet service providers, and searchengine and social media companies);

- E. Strengthen the international framework (1) to establish more efficient mechanisms of transnational cooperation among nations and private

actors, and, if possible, (2) to procure a greater uniformity among national legislations;

- F. Work on a regulatory and adjudicatory model based on the co-responsibility of private and public actors, and on multiple regulatory and conflict-resolution approaches. Such model might include at least four strategies, all of them able to constantly adapt to the ever-changing environment of the internet and communication technologies:
  - Promote further research and cooperation among electoral authorities, academics and practitioners in order to assess the real impact of digital technologies on electoral processes and the efficiency of the adopted measures;
  - Foster education to strengthen legal and democratic culture among citizens;
  - Promote self-regulation, like the mandatory adoption of ethics and corporate social responsibility codes, among internet service providers, and search-engine and social media companies; and
  - Provide remedial mechanisms in laws, policies and alternate conflict resolution mechanisms.

150. At the level of the Council of Europe, much has already been done to meet the abovementioned challenges. Inter alia, the Budapest Convention provides for a range of tools for the prevention of cybercrime – including during the electoral process – and for international cooperation aimed at securing electronic evidence; importantly, current works on a 2nd Additional Protocol to the Convention should permit added options for enhanced international cooperation and access to data in the cloud. Furthermore, a series of legal standards are in place for the protection of privacy and personal data in the context of social media. In particular, the Modernised Convention on the protection of individuals with regard to automatic processing of personal data, which is open to any country in the world and which sets international standards, should serve as the universal treaty for data protection. Finally, a number of legal instruments have been developed to ensure free elections, in particular through electoral campaign funding regulations and measures to prevent inequality in media coverage during elections both online and offline.

151. At the same time, several Council of Europe documents suggest that there is room for further improvement. In particular, the CoE Information Disorder Report 2017 made a number of recommendations directed at governments, education ministries, media organisations, technology companies and civil society to address the challenges posed by the increasing mis-, dis- and mal-information and their impact on democratic processes; and the CoE Election Study 2017 concluded that the current regulatory framework no longer suffices for maintaining a level playing field for political contest and for limiting the role of money in elections, and it suggested a number of measures to remedy this situation.

152. Taking the main results of these documents and of the present study into account, the recent shift in the influence of internet-based channels of electoral communication calls for action in the following areas:

- A. Revision of rules and regulations on political advertising: in terms of access to the media (updating broadcasting quotas, limits and reporting categories, introducing new measures covering internet-based media, platforms and other services, addressing the implications of micro targeting) and in terms of spending (broadening of scope of communication channels covered by the relevant legislation, addressing the monitoring capacities of national authorities);

- B. Accountability of internet intermediaries in terms of transparency and access to data enhancing transparency of spending, specifically for political advertising. In particular, internet intermediaries should provide access to data on paid political advertising, so as to avoid facilitating illegal (foreign) involvement in elections, and to identify the categories of target audiences.

- C. Quality journalism: strengthening of news accuracy and reliability, enhanced engagement with the audience, strengthening of public service media and local media, and empowering self-regulation with an added focus on transparency of online news and their circulation;

- D. Empowerment of voters towards a critical evaluation of electoral communication targeted action for preventing exposure to false, misleading and harmful information (with due reflection on the limits of fact-checking initiatives; efforts on media literacy (including social media literacy) through education and advocacy;

- E. Open internet: ensuring net neutrality, considering legally strengthening users' rights to an open internet, and ensuring that any restrictions on access to internet content are based on a strict and predictable legal framework regulating the scope of any such restrictions, and ensuring that judicial oversight to prevent possible abuses is guaranteed;

- F. Data protection: affirming and protecting the right to anonymity on the internet, regulating and strictly limiting the creation and use of profiles, in all kinds of different contexts. In addition, the Council of Europe might consider adopting guidelines on the restrictions to be imposed on surveillance technologies, including the international trade in such technologies; promoting Convention 108 as the "gold global standard"; and possibly developing a specific legal instrument to address the high risk that the use of digital technologies in political campaigns and advertising represents to personal data protection.

153. As stressed earlier, the borderless nature of the internet and the private ownership of the information highways render the current challenges to democracy and electoral processes particularly complex. International cooperation and involvement of the relevant private actors are therefore indispensable to face these challenges and to ensure the right to free elections and the functioning of democracy in the future.

NOTES

Council of Europe member states undertook *"to hold free elections at reasonable intervals by secret ballot, under conditions which will ensure the free expression of the opinion of the people in the choice of the legislature".*

Protocol to the European Convention on Human Rights,
Article 3: Right to free elections

"Artificial Intelligence raises important and urgent issues. AI is already with us – changing the information that we receive, the choices that we make, and the ways in which our societies function. In the coming years AI will play an even greater role in the way that governments and public institutions operate, and the way in which citizens interact and participate in the democratic process".

Marija Pejčinović Burić
Secretary General of the Council of Europe

This compendium is a collection of different Council of Europe documents which comprises standards and recommendations to the member States on how to ensure right to free elections enshrined in the European Convention on Human Rights in the era of digital technologies and AI. The compendium will be updated on a regular basis with relevant Council of Europe documents and instruments, once they are developed and adopted.

www.coe.int

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

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE