Prof. Dr. Thomas Schmitz[1] Kazakh-American Free University, 11.04.2024

New Threats for Democracy in the Era of Digitalisation

I. Introduction

1. Democracy in decline worldwide
   a) The global rise of anti-democratic populism
      - populist movements, parties and politicians trying to destroy democracy from within
      - a serious threat to democracy,[2] to young democracies (e.g. Indonesia) as to those with long tradition (e.g. USA)
      - especially - but not only - a crisis phenomenon of the West
      - latest: the tendency of right-wing populists, triggered by Donald Trump, to accept election outcomes only if they win (USA 2020, USA 2022, Brazil 2022/23)
   b) The short way from democracy to autocracy under a populist government
      - Turkey, Hungary, Poland, Philippines, attempts in Slovenia, Slovakia, Brazil and by Donald Trump in the USA...
      - see my course paper "How to become a dictator - a practical instruction"
      - latest in Germany: mass deportation plans of a right-wing populist party represented in parliament against foreign nationals and German citizens with migration background
   c) Russia's and China's war on democracy
      - Russia's systematic support of anti-democratic populists and far-right extremists in Europe and North America
      - Russia's war on Ukraine and threats against other East European democratic states - a war against the basic concepts of democracy and self-determination of peoples
      - China's crackdown on democracy in Hong Kong, threats against democratic Taiwan, support of autocratic rulers in Southeast Asia (Myanmar, Cambodia) and propagation of the "superior" totalitarian Chinese system of rule
2. The return of the dominance of lie and propaganda in the public discourse
   - a massive dissemination of lies and propaganda by smart use of digital media, often disguised and well-coordinated, ending a period of decades of more mature, fact-oriented public discussion in many democratic states
   - distorts the public discourse and devalues it in its essential role for a functioning democracy
3. The growing polarisation of democratic societies
   - heated, emotionally charged debates in a divided and agitated, partly radicalised society make constructive, rational public discourse, as democracy needs it, increasingly difficult, tearing apart even couples and families
4. The threat of deglobalisation further destabilising young democracies
5. Backgrounds
   - the *legacy of 30 years of neoliberalism*, neglecting social cohesion and the interests of the ordinary people
   - the *side effects of globalisation*, which produces everywhere not only winners but also losers
   - *angry old (white) men*, *defending their unjustified privileges*, unwilling to adopt to the changing world
     - unable to cope with cultural changes, changing morals and the rise of women and minorities in society
     - not only *white* men are the problem...

II. New threats to democracy related to the electronic media

1. Hate posts in the internet
   - online attacks on personal honour and dignity, often denigrating the victim on the basis of gender, age, ethnic background, religion, sexual orientation or physical characteristics
   - mostly from the cover of the anonymity of the internet - the perpetrators would not dare to act like that offline...
   - the *"shitstorm" - symbol for* the discussion culture of *our time?*
2. Cyberbullying and cyberintimidation
   - new, highly effective means of harassment and coercion in the era of digitalisation
   - can go as far as threats of rape or murder and public incitement to commit such crimes
     - particularly dangerous, as they may be implemented independently from the will of the agitator
   - *often targeted against intelligent, politically active young women* in order to silence them in the public discussion
   - also used to stifle academic discussion: the 2020 case of *death threats against the Constitutional Law Society at Universitas Gadjah Mada (Yogyakarta)* over a planned online discussion on presidential impeachment

---

[1] DAAD Lecturer in Law at Maqsut Narikbayev University, Astana; Außerplanmäßiger Professor (adjunct professor) at the University of Göttingen; www.thomas-schmitz-astana.kz, www.thomas-schmitz-yogyakarta.id, www.jura.uni-goettingen.de/schmitz, www.thomas-schmitz-hanoi.vn, http://home.lu.lv/~tschmit1; E-Mail: tschmit1@gwdg.de.

[2] Underlined text passages indicate links to relevant internet resources. Just click on the link in the pdf file!

3. Intimidation of the citizen by government control of his conduct via internet- and app-based social credit score systems
   - digital means for a totalitarian "soft" control of the citizen, to ensure conformist behaviour and suppress unwanted criticism
     - a first beginning: the *Social Credit System in China*
   - utilising apps and websites, bookings and credit card payments, the citizen's smartphone, computer and tv and potentially even cameras, microphones and other electronic systems in public spaces and buildings to spy on him
   - using the extensive personal data collected for a continuous social assessment and evaluation of the citizen with concrete consequences for his professional, private and social life
4. Government control and "nationalisation" of the internet
   - attempts to decouple, even physically, the national part from the global internet, in order to enable full government control and censorship
     - the example of Russia
   - bans on global social media and promotion of easy-to-control domestic alternatives
     - the examples of Russia and China
5. The biggest threat: dissemination of fake news and organised disinformation campaigns
   - directly targeting the foundations of a rational, fact-based public discourse
   - an old phenomenon revived by the general availability and wide reach of the digital media
   - an approach often used by rich stakeholders and foreign governments who act covertly through controlled media and lobbyist group, but in the digital era open to everyone
     - now facilitated by the use of artificial intelligence (e.g. *ChatGPT*)
   - often not aimed to convince of the false allegations but rather to *undermine the trust in any information*, in order to neutralise the effect of correct information in trustworthy media
   - topic problems: *foreign election interference* and disinformation related to the Russian war of aggression on Ukraine
6. Manipulation of the public discourse by social bots
   - software agents communicating autonomously on social media and internet platforms (commenting, liking, retweeting, chatting etc.), usually operating undercover, feigning personal communication by a human being
     - the "personal comment" on journalistic articles or in Facebook posts is often that of a machine
   - massive use under different user names feigns a broad public resonance or a widely shared opinion
     - the apparently "prevailing opinion" in the digital media is often that of a small minority
7. Manipulation of the public discourse by distorted online opinion surveys
   - opinion polls on media sites are not representative and thus misleading, since they
     - only reflect the opinions in the specific group of the media site's readers
     - can be easily influenced by concerted actions of activists
     - may even be manipulated by social bots
   - without further clarification, they distort the process of forming public opinion

III. How to respond to the new threats to democracy? A selection of practices and ideas

1. Raising awareness of the need to protect the integrity of the democratic process
   - democracy is not stable by itself, not even in countries with a long democratic tradition
   - the democratic process is by nature vulnerable to manipulation by undue pressure and deception
   - the need to revive the *concept of "defensive democracy"* of KARL LOEWENSTEIN
2. An institutional guarantee of a free and open but unmanipulated internet
   - a special guarantee in the national constitution (for the national part of the internet) and/or in an international treaty
   - must include the *freedom of the internet as such* from unjustified government control
   - must prohibit any "nationalisation" (forced isolation of the national part) of the internet
   - must require *protection of the integrity of the internet* against manipulative techniques and practices (see infra, 6)
3. A priori exclusion of proven false allegations of facts from the freedom of expression and other communicative freedoms
   - by reinterpretation or reformulation of the respective clauses in human rights treaties and constitutions
   - inspiration from the positive German experience with the restrictive interpretation of the scope of protection of the freedom of opinion (art. 5(1) phrase 1 of the German Basic Law) by the Federal Constitutional Court[3]
   - the idea: proven false allegations of facts (especially lies) can only be destructive in the formation of opinions and thus in the democratic process and therefore should not be protected at all by the communicative freedoms
   - a precaution to facilitate the intervention of authorities and courts against disinformation
4. Fact checking and public exposure of fake news
   - a valuable contribution of journalists and the civil society in special portals and journalistic formats
   - can support the intervention of authorities and courts against disinformation

[3] See especially the famous decision on the holocaust denial, Federal Constitutional Court, 13.04.1994, 1 BvR 23/94, B.II.1.b (BVerfGE 90, 241, 247), English translation of excerpts at https://law.utexas.edu/transnational/foreign-law-translations/german/case.php?id=621, with further references.

5. Specialised police departments, prosecutor's offices and civil society organisations for a more efficient but transparent fight against hate posts, cyberbullying and cyberintimidation
   - with specially trained digital media experts
   - providing support to the victims and expediting the law enforcement
   - however, transparency of their work must be ensured to avoide abuse

6. Special precautions against the manipulative anti-democratic abuse of the internet
   - in particular stricter rules for internet platforms and social media

   a) Rules *ensuring the identifiability of users* of internet platforms and social media
      - e.g. by requiring the deposit of verified identity data with the provider
        - access of authorities to these data should require judicial approval
      - e.g. by requiring the use of real names in public discussions

   b) *Strict liability (liability without fault) of social media providers* for encroaching content on their platforms
      - the most effective way to make providers comply with their responsibility
      - providers are not innocent but operators of an extremely dangerous and harmful machinery who must bear its risk
      - proposal: victim must gain *civil compensation in the form of a lump sum* in a quick and simplified prodecure *directly from the provider*, who then may have recourse against the responsible user
      - also helpful but not enough: the *new obligations of providers under the EU Digital Services Act* (regulation 2022/2065)
        - hosting services and online platforms must operate *notice and action mechanisms* where users can notify illegal content; they must process the notice timely and remove or disable access to illegal content
        - in case of suspicion of certain crimes, they must notify it to law enforcement authorities
        - users can seek compensation for violations of these rules

   c) Legally *binding standards for algorythms* to prevent a destabilising extreme polarisation of the society
      - in particular prohibition to favour provocative posts with extreme views or style to attract attention

   d) A general, punishable *ban on social bots* (or at least the diguised use of them)
      - no tolerance for deceptive means to fake public resonance or interpersonal communication!
      - in particular: strict ban on the use of social bots by political parties and in electoral campaigns
      - in particular: measures against social bots used by foreign governments for disinformation campaigns
      - social bots in business life must be limited to exceptions, require disclosure and not be allowed for public debates

   e) Mandatory *transparency rules for online opinion surveys*
      - requiring information about the time or period of the survey and the number and selection of participants, to allow a realistic assessment of the degree of "representativeness"

   f) One-stop online complaint offices
      - where citizens can report violations easily and unbureaucratically to the authorities
      - may cooperate with the specialised police departments, prosecutor's offices and civil society organisations (see supra, 5)

   g) Enhancing the citizen's awareness for the risk of manipulation, by education and training
      - not only in schools but also for the elderly and less educated citizens
      - urgently needed in Western countries: effective immunisation training against internet-spread conspiracy theories

7. International cooperation of democratic states to reconcile the protection of the communicative freedoms with the need to protect against their abuse

   a) An *international treaty on cooperation in the defence of democracy*
      - open only to democratic states (who will not try to sabotage it) but offering support also to others
      - establishing international institutions, such as an independent *expert treaty body*, institutionalised *forums*, or even a *specialised human rights court* (for legal protection in serious cases or questions of general interest)
        - see already the example of the Council of Europe, which focuses, however, on democracy in Europe
        - see already the example of the African Charter on Democracy, Elections and Governance, which focuses, however, on basic questions of democracy in Africa
      - establishing ***international control mechanisms*** to ensure that the instruments for the protection of democracy will not be misused to destroy it (a purely national solution without intern. accountability would be too risky)

   b) International elaboration and further development of *universal democratic standards* for both, the protection of the communicative freedoms and the protection against their abuse
      - detailed standards to facilitate a constructive and rational, broad and open, non-hierarchical public discourse
      - especially *universal standards for a free civil society*
      - continuous development of these standards with regard to new challenges in thematic forums, involving political and legal science and the civil society

   c) Promotion of the transcultural international dialogue on the conditions and requirements of democracy
      - a broad and open international discourse may be the most promising way to maintain freedom but avoid abuse

8. Last but not least: defence of pluralism and tolerance as essential conditions for democracy
   - democracy requires a *broad and open public discourse* in a *pluralistic culture* that brings together different stakeholders and different political, ideological and moral approaches and worldviews in a constructive debate; mutual respect and tolerance are essential preconditions for that
   - the free public discourse must be defended, if necessary even by the *sharp instruments of defensive democracy* - *no tolerance for intolerance* - not even in the digital media!

IV. Conclusion

- digitalisation is not the reason for the contemporary worldwide decline of democracy but acts as a dangerous accelerant
- to preserve democracy, first of all the real reasons, especially the *social divide*, *need to be addressed*
- moreover, the mechanisms of defensive democracy need to be deployed and, where necessary, enhanced
- there is a *large catalogue of promising measures* against the specific threats emanating from digitalisation, but they need to be developed continuously; for this and to prevent the risk of abuse, a *broad* and *transcultural institutionalised international cooperation of democratic states in the defence of democracy* is necessary
- the measures against the new threats for democracy bear the risk of threatening democracy itself; international control mechanisms can help to ensure that this risk does not materialise

Further Reading

Brkan, Maja: Artificial Intelligence and Democracy: The Impact of Disinformation, Social Bots and Political Targeting, Delphi - Interdisciplinary Review of Emerging Technologies 2 (2019), no. 1, p. 66 ff., https://doi.org/10.21552/delphi/2019/2/4

Dan, Viorela; Paris, Britt; Donovan, Joan; Hameleers, Michael; Roozenbeek, Jon; van der Linden, Sander; von Sikorsk, Christian: Visual Mis- and Disinformation, Social Media, and Democracy, Journalism & Mass Communication Quarterly 98 (2021), p. 641 ff., doi.org/10.1177/10776990211035395

European Parliament, Panel for the Future of Science and Technology (STOA): Liability of online platforms, 2021, www.europarl.europa.eu/stoa/en/document/EPRS_STU%282021%29656318

Hendricks, Vincent F.; Vestergaard, Mads: Reality Lost. Markets of Attention, Misinformation and Manipulation, 2019, doi.org/10.1007/978-3-030-00813-0

Hong, Matthias: Regulating hate speech and disinformation online while protecting freedom of speech as an equal and positive right - comparing Germany, Europe and the United States, Journal of Media Law 14 (2022), no. 1, p. 76 ff., doi.org/10.1080/17577632.2022.2083679

Hollies, Duncan B.; Ohlin, Jens David: Defending Democracies. Combating Foreign Election Interference in a Digital Age, 2021, doi.org/10.1093/oso/9780197556979.001.0001

Keller, Tobias R.; Klinger, Ulrike: Social Bots in Election Campaigns: Theoretical, Empirical, and Methodological Implications, Political Communication 36 (2019), p. 171 ff., doi.org/10.1080/10584609.2018.1526238

Maldonado, Manual Arias: The internet against democracy, Eurozine 15.10.2017, www.eurozine.com/the-internet-against-democracy

Rettinger, Lizzy: The Human Rights Implications of China's Social Credit System, Journal of High Technology Law 21 (2021), no. 1, p. 1 ff., https://sites.suffolk.edu/jhtl/files/2021/01/Rettinger.pdf

Stadnik, Ilona: Russia. An independent and sovereign internet?, in: Blayne Haggart; Natasha Tusikov; Jan Aart Scholte (editors), Power and Authority in Internet Governance. Return of the State?, 2021, Chapter 7, https://doi.org/10.4324/9781003008309

See also the Special Issue of the *Election Law Journal*: Foreign Election Interference: A Global Response, vol. 20 (2021), no. 1, www.liebertpub.com/toc/elj/20/1