ie UNIVERSITY
CENTER FOR THE GOVERNANCE OF CHANGE

TECH4DEMOCRACY

DEMOCRACY-AFFIRMING TECHNOLOGIES

ALIGNING TECHNOLOGY WITH PUBLIC INTEREST AND SOCIAL GOOD

JUNE 2023

US department of State legal disclosure [PENDING]

Members of the Tech4Democracy Advisory Board:

- Marcelo Cabrol, Chief of the IDB Lab's Scalability, Knowledge and Impact division at the Inter-American Development Bank

- Alicia García-Herrero, Senior Research Fellow, Bruegel; Professor, Hong Kong University of Science and Technology

- Amy Larsen, Director of Microsoft's Democracy Forward initiative

- Susana Malcorra, former Foreign Minister of Argentina; former chief of staff to UN Secretary-General Ban Ki-moon

- Manuel Muñiz, Provost, IE University; Dean, IE School of Global and Public Affairs; Chair, IE Center for the Governance of Change

- Allison Peters, Senior Advisor to the Under Secretary of State for Civilian Security, Democracy, and Human Rights

- Glen Weyl, Head of Web3 research at Microsoft; author; Founder of RadicalxChange

Contributors to this report:

- Tyson Barker, Senior Advisor at the Bureau of European and Eurasian Affairs in the US Department of State

- Irene Blázquez-Navarro, Director at the Center for the Governance of Change, IE University. She is a legal scholar and international lawyer by training, as well as a specialist in strategy, security, defense, and technology. She previously served as Adviser to the State Secretary for Global Spain (Ministry of Foreign Affairs) and as Head of the Strategic Planning Office (National Security Department – Spanish Prime Minister's Office) between 2012 and 2020

- Elisabeth Braw, senior fellow at the American Enterprise Institute (AEI), where she focuses on defence against greyzone threats. She is also a columnist with Foreign Policy and Politico Europe, as well as a member of GALLOS Technologies' advisory board and a member of the UK National Preparedness Commission

- Maria Paz Canales, lawyer from the University of Chile and holds a Master's in Law and Technology from the University of California, Berkeley. She was part of the team that founded Derechos Digitales, a Chilean based independent non-profit organization, working since 2005 for the protection and promotion of human rights in the digital environment in Latin America. Between 2017-2021 she was Derechos Digitales' Executive Director and she is currently the Head of Legal, Policy and Research for Global Partners Digital a social purpose company working to enable a digital environment underpinned by human rights

- Jeremy Cliffe, Writer at Large at the New Statesman and Future World Fellow at the IE Center for the Governance of Change

- Cathryn Clüver Ashbrook, Executive Vice President/Senior Advisor at the Bertelsmann Stiftung in Berlin, Germany. She previously served as the Director and CEO of the German Council on Foreign Relations (DGAP) and for over a decade as the Founder and Executive Director of the Future of Diplomacy Project at the Harvard Kennedy School, following earlier, senior roles in European think tanks, policy advisory and international journalism

- D.J. Flynn, Assistant Professor of Political Science and Faculty Affiliate at the Center for the Governance of Change at IE University in Madrid, Spain. His research uses experiments and statistics to study misinformation, public opinion, and political behavior. Before joining IE, he received his PhD in political science from Northwestern University and completed a postdoctoral fellowship in quantitative social science at Dartmouth College

- Darío García de Viedma, Associate Director at the Center for the Governance of Change, IE University. He formerly worked as a Product Manager in the tech industry. He has been trained in Political Science at Sciences Po, with a MSc in Social Research Methods at the London School of Economics

- Daniel Innerarity, Professor of Political Philosophy. Researcher of the Ikerbasque Foundation for Science at the University of the Basque Country and Chair Artificial Intelligence & Democracy at the European University of Florence

- Marcin Kilanowski, Prof. NCU dr hab. Marcin Kilanowski LL.M. (Harvard). Experienced academic with strong interest in the field of policy and law formation in national and global setting. Visiting scholar, Professor and Visiting Professor at universities in Poland and abroad (Harvard, Oxford, Science Po, Freie Univerrität, Goethe-Universität), and then as a founder of think-tanks and an expert and advisor to ministerial councils and international organizations like United Nations Global Compact

- Peter Loewen, Director of the Munk School of Global Affairs & Public Policy, Associate Director of the Schwartz Reisman Institute for Technology and Society, Robert Vipond Distinguished Professor of Democracy in the Department of Political Science at the University of Toronto. He is also the Principal of OpinionAI, a private consulting firm conducting research on attitudes towards AI and technology

- Trisha Ray, Fellow and Deputy Director at the Center for Security, Strategy and Technology at the Observer Research Foundation in India. Her research focuses on geopolitical and security trends in relation to emerging technologies. Trisha is a member of UNESCO's Information Accessibility Working Group, a Pacific Forum Young Leader, an AI Connect Fellow as well as a 2022 Schmidt Futures ISF Asia Fellow

- Alejandro Roche, Associate Director at the Center for the Governance of Change, IE University. Former corporate attorney and strategy consultant, with over 12 years of international experience in the private and nonprofit sectors, specialized in global affairs, public policy, emerging technologies, sustainable development, campaigns for social change and human rights

- José Ignacio Torreblanca, Head of Madrid Office and Senior Policy Fellow at the European Council on Foreign Relations (ECFR)

Table of content

FOREWORD

Irene Blázquez-Navarro

This report is an integral component of Tech4Democracy, a global initiative led by IE University in partnership with the U.S. Department of State that was incorporated into The Summit(s) for Democracy launched in 2021 by President Biden. The initiative showcased its achievements in March 2023 at the Second Summit for Democracy in Washington, DC.

Many academic institutions, think tanks, and other organizations joined this ambitious effort to harness the power of technology for social good that became a tangible reality thanks to Microsoft's strategic support.

The ultimate goal of Tech4Democracy is to engage different communities—international organizations, governments, businesses, innovators, investors, academia, and civil society as a whole —to strengthen our democracies through technological innovation and actively address the future needs of our political systems.

The first key goal of Tech4Democracy is to raise awareness about why democracy matters in an age of absolute technological disruption. A prime example is the swift deployment of OpenAI's ChatGPT, a Sputnik moment in the technological race. It is critical that we appreciate how emerging technologies have profound implications not only on prosperity, but also on the balances of power, the guiding principles of politics, the determinants of peace and security, and how we understand "humanity".

This is particularly important in an era when autocrats, nationalists, and populists around the world are gaining prominence. These groups are exploiting rapid changes brought by new technologies to undermine democratic systems and processes. As has been said by so many: Technology favors tyranny. Much has been written and discussed about how "in the coming few years either tech will destroy democracy and the social order as we know it, or politics will stamp its authority (…), [such that it is] becoming increasingly clear that technology is currently winning this battle (…)."[1] Some experts raise concerns that emerging and disruptive technologies will do more for autocracy than for democracy. They argue that autocracies are unconstrained by "regulation with teeth" on privacy, data protection, equality, inclusion, or tech literacy and exemplify how technology and AI can work to support democracy. [2]

Critical thinking about technology capabilities is all the more crucial and acquires growing relevance in social and democratic states governed by the rule of law. They are assets to be preserved and, probably in the near future, legally protected. Liberal democracies can leverage and generate citizen trust across diverse regional latitudes and work together with an empowered civil society, including academia, and an engaged private sector guided by the SDGs and ESG principles. Such technologies as AI will automatically convert unstructured information into actionable knowledge. But wisdom, as well as consciousness, will always belong to a tech-literate citizenry.

In an era of revisionism of the international liberal order and great competition for power, democracies must be able to revamp and effectively deliver to their citizens. This imperative becomes all the more critical as technology emerges as not only a distinct domain within international relations, but also one that significantly shapes a unique framework of international law and diplomatic relations. Such a framework is poised to take shape, mirroring the ongoing development of international environmental and climate law.

But "revamping democracy" remains a hollow phrase. Questions about how to modernize democracies and ensure not only "tech4democracy" but also "democracy4tech"[3] remain vital. Throughout history, democracies have consistently led in the provision of global public goods and have enhanced freedom, security, and prosperity for their citizens. Ensuring that the prevailing law accurately reflects the general will of the people is key to this success. Democracies also uphold the principle of legality that guarantees the division of powers. Public authorities' actions are subject to independent judicial control to prevent arbitrary overreach. Additionally, democracies prioritize the legal protection and effective realization of fundamental rights and freedoms.[4] How can our current democracies deliver and make progress as successful political system in a context of technological disruption?

This question informs the second main goal of the Tech4Democracy initiative: developing specific strategies to strengthen democracy through the use of technology. This approach not only embraces technological disruption, but also anticipates areas where technology can effectively enhance such democratic principles as checks and balances, respect for political rights and civil liberties, and informed debate.

Tech4Democracy aims to imbue "democracy-affirming technologies" with substance as well as actionable and enforceable qualities. This fresh concept born from the launch of the Summit for Democracy in 2021 presented a tremendous opportunity for those of us operating at the intersection of technology and policy, whether in government, private sector, entrepreneurial ventures, academia, or social media. To map the boundaries of democracy-affirming technologies for the very first time, we made the deliberate choice to launch this process within a distinctive space: entrepreneurship and innovation. This space serves as an ideal barometer for significant change trends and allows us to capture the pulse of emerging trends.

The entrepreneurship space, as beacon of change, provided valuable insights and outcomes to identify and refine the essential components of this emerging concept. In a sector teeming with talent where creatives and pioneering minds converge, technology intertwines with the pursuit of knowledge and the creation of transformative societal spaces. IE University holds the distinguished rank of fourth globally and first in Europe in the field of entrepreneurship and innovation, so it was only natural that this exercise should start there.

Between 2022 and 2023, Tech4Democracy conducted a Global Entrepreneurship Challenge to select promising innovators committed to fostering technology for social good through competitions (Venture Days) held on all five continents. Utilizing this sample as a foundation, we have built the initial framework for the category of democracy-affirming technologies. More than 300 startups from 66 countries participated in the Global Entrepreneurship Challenge and attended competitions in Madrid, Bogota, Stanford, Delhi, and Cape Town. Prominent academics, thinkers, and investors joined the juries. Featured keynote speakers included Jacinda Ardern, former Prime Minister of New Zealand, Samantha Power, Administrator of USAID, and Vitalik Buterin, Founder of Ethereum.

The framework is informed by the experiences of the Global Entrepreneurship Challenge and the drafting of the report itself. It is, moreover, consistent with the liberal principles of technological humanism and the principles of progress, innovation and justice that it enshrines. A technological humanism means placing individuals and their fundamental rights and freedoms at the center and making them the unit by which both the progress driven by new technologies and the challenges they pose are measured.

To contribute to the crystallization of this category, we propose the comprehensive definition that encompasses both procedural and finalistic aspects as well as the entire life cycle of the technology, starting from its ideation phase through implementation and reaching its peak, the purpose and utilization of the technology, and the effects it generates, with particular emphasis on unintended consequences and existential risks:

Democracy-affirming technologies are intentionally designed, developed, and deployed to actively promote and uphold a set of fundamental values, principles, and rights. These essential components encompass the right to liberty and personal autonomy, the protection of privacy and private data, the principles of inclusion and equitable access, the dissemination of truthful information, the fostering of citizens' tech critical thinking, the utilization of technology to enhance legislative bodies, participation in free elections, the separation of powers, the principle of legality, and the safeguarding the rule of law.

A scrutiny of the suitability, ability, and capacity of these technologies to promote these pillars will be required and could well follow the model of international standards developed and certified by the International Organization for Standardization.

At a crucial juncture marked by such impending regulations as the approval of significant measures like the EU AI Act the precise delineation of categories of this cross-cutting and encompassing nature remains to be determined. These categories span across the various political systems, each with their own distinct regional priorities and technology diplomacy agendas.

Were *democracy-affirming technologies* to establish a foundational framework that garners a resolute and robust international consensus and were the Tech4Democracy community to continue to flourish with the significant momentum of recent accomplishments, we could then forge ahead to progressively identify and refine the essential components of these technologies. This, in turn, would provide a valuable benchmark of best practices for all the communities mentioned in this foreword at their different levels of competence, responsibility, and commited interest.

Moreover, democracies should cooperate to establish a shared set of rules and norms pertaining to new technologies. This would lay the groundwork for a Universal Declaration of Human Technology Rights fostered under the auspices of the United Nations and upheld by a global monitoring agency.

A new plan is needed to adapt democracy to tech and vice versa: new global governance and regulation, new codes of conduct for the tech industry, new rights and obligations, and new public agencies, bodies and institutions.[5]

Efforts should be directed toward devising effective strategies to bridge the gaps created by rapid technological advancements that often outpace the finely tuned responses of democratic societies. Simultaneously, there is a need to prioritize the application of cutting-edge, emerging, and disruptive critical technologies to key sectors that require institutional commitment and reinforcement to serving the ultimate purpose of delivering social good.

This report contributes to the two main objectives of the Tech4Democracy initiative, namely to raise awareness about why democracy matters and to develop specific strategies to strengthen democracy through the use of technology that cultivates informed situational knowledge about the importance of fostering a future for democracy in an era of technological disruption. The report also includes a summary of the continental competitions held to identify “innovators for democracy” around the world, a *Tech4Democracy Radar*. We were moved by the desire to establish synergies between awareness and avenues of action.

Both the Tech4Democracy initiative and this report date in their origin and related development to the end of 2021. They do not address head-on the "constitutional moment" that the foundation models, including generative AI, have brought about since March 2023. Another key issue in the current debate is left out of this document. I refer here to the *digital public infrastructures*, with an estimated eight distinct attributes for providing *global public goods:*[6] enabling SDGs, inclusive, citizen-centric, trustworthy, supportive of innovation, interoperable, resilient, and politically viable.[7] Finally, the report flags a window of opportunity to summon voices from democracies around the world in the future when heretofore in geopolitics the focus has been given to the Euro-Atlantic vision.

The report begins with an introduction by Jeremy Cliffe. Working from the premise that all technology is human, Cliffe explores the increasing divisions in democratic societies. His thesis contends that democracy-affirming technologies are surprisingly under-explored, and he cites the Tech4Democracy - Global Entrepreneurship Challenge as a model for technologies and applications that can support democratic resilience. Cliffe reminds us that there is such verve and originality out there that the challenge lies in harnessing these for the task at hand.

The frontispiece of the introduction and backbone of this report is the Tech4Democracy Radar developed by Darío García de Viedma and Alex Roche. This radar uses the international sample from the startup ecosystem to show how the sector is using existing technologies to build applications that support democracy. The authors observe that there is no deliberate effort to create democracy-affirming technologies per se. This leads them to consider a wide range of interpretations about the potential risks and opportunities that come with the ongoing development and establishment of democracy-affirming technologies. Sixteen categories of technologies with a varying degree of sophistication (NLP, DLT, ML, quantum computing, AR, VR, etc.) are taken into account and are measured in light of the patents they are granted. García de Viedma’s and Roche’s essay is sure to insightful and raise further proposals.

After this introduction, the report unfolds in two sections on the governance of technology and the rights that technology has to strengthen to foster the technological humanism discussed above. It concludes with a piece on the new social contract required by this technological transformation. “Geopolitics, Governance and Diplomacy of Technology: Recent Trends” comprises contributions by Cathryn Clüver Ashbrook, Ignacio Torreblanca, Tyson Barker, Maria Paz Canales, and Trisha Ray.

Clüver opens with the big picture: technology is becoming the frontline of geopolitical competition and control. She presents us with avenues for the governance of technology that advocate, *in toto*, a "patched and ‘nodalized’ governance structure" instead of a wider governance structure. Subsequent contributions are a logical continuation of Clüver's portico that deepen and explore the discussion of how technological governance will be shaped in the context of accelerating rivalry between democracies and autocracies.

These are rich essays because of the diversity they represent in their regional approach and, thus, to a large extent, "principled" approach. Torreblanca, asks us an always topical question (especially for convinced pro-Europeans such as myself) in connection with Cliffe's presentation of statistics on the decline of democracy: Is the EU a force for (digital) good?

Barker continues with an essay on the EU/USA transatlantic relationship as mediated by the Trade and Technology Council (TTC), where technological issues that go beyond the "trade" label are settled; this is always the deciding body when it comes to technology because it crosses all domains, including security and defense, politics, and prosperity. The fourth summit of the TTC in Sweden, May 30-31, addressed an AI roadmap and a warning mechanism for disruptions in semiconductor supply chains.

The chapter also incorporates a regional perspective. Canales draws attention to the need to re-balance the relationship between north and south to ensure the protection of digital rights across the globe. Here, this global south refers to any stakeholder from less developed countries that are in majority, but not exclusively, located in the southern hemisphere. As Canales underlines, most of the world's inhabitants are located in those jurisdictions.

The first section ends with Trisha Ray's thesis: there is a limiting Eurocentric, Americentric perspective about what the "correct" practice of democracy should be. She discusses how digital technologies have improved government service delivery, enhanced transparency, enabled wider political participation, and provided spaces for underrepresented voices in Asia.

The second section, "Deployment and Regulation of Technology to Ensure Rights," is more closely tied to the overarching vision of technological humanism that forms the foundation of the suggested approach to the concept of democracy-affirming technologies. Contributions by Daniel Innerarity, D.J. Flynn, Marcin Kilakowski, and Peter Loewen, highlight that data, truthful information, and tech literacy are core elements that must be addressed by *democracy-affirming technolo*gies.

Innerarity argues that the resilience of politics as a human activity cannot be replaced by technology, though it should undoubtedly benefit from it. In this sense, Flynn addresses the role of an informed public in democratic systems and argues that its functioning depends in large part on an informed citizenry. He also discusses three recent changes in the information environment: media fragmentation and selective exposure; social and media polarization; and fake news and opinion distortion.

Two successive pieces can be read as the flipped sides of a coin. Whereas Kilanowski deals with a series of rights of the citizen, namely right to truth, right to privacy, and right to know, Lowen puts argues that public authorities need to understand the preferences of their administrators to democratically deliver. Governments should know as much about what citizens want and think as possible such that they can perform better. Lowen distinguishes between this goal and a surveillance State.

Elisabeth Braw's essay on "The Need for a New Social Contract" is included as a conclusion. As the author explains, technological transformation has created a new empowered citizen who must be heard through various platforms.

As a coda, I would like to stress that Tech4Democracy is a global initiative aimed at leveraging technology to defend and promote democracy today and for future generations. The urgency of our call to action has become clear with recent events, including the aggression against Ukraine. If democracies must revamp in an era of great power competition with autocratic regimes, then technology must play a significant role.

Technology drives the world at an unprecedented speed. This can be for the better if properly guided and governed. It is up to us to anticipate how the use of technology can serve our rights and principles and to determine the steps that need to be taken to guarantee that democracy as a political system thrives.

Time is of the essence, and we all have a crucial role to play. If we want democracy to succeed in continuing to deliver global public goods, we must align technology with the best interests of humankind and build alliances that mobilize the tech for social good and progress for geopolitical leadership.

Endnotes

[1] Bartlett, J. (2018). The people vs tech.

[2] Buchanan, B. & Imbrie, A. (2022). War, peace, and democracy in the age of artificial intelligence.

[3] Azhar, A. (2021). The exponential age: How accelerating technology is transforming business, politics and society.

[4] Díaz, E. (1966). Estado de derecho y sociedad democrática.

[5] Susskind, J. (2022). The digital republic: On freedom and democracy in the 21st century.

[6] Hubbard, S., Moore, S., Rong, H., & Trivedi, A. (2023). Fostering a Digital Commons: Internet-Native Experiments For Sustainable Open-Source Software. Perspectives on Public Purpose.

[7] Chakravorti, B. (2023). The case for investing in Digital Public Infrastructure. *Harvard Business Review.*

INTRODUCTION: TECH FOR DEMOCRACY AND DEMOCRACY FOR TECH

1. Democracy Today and in the Future.

Jeremy Cliffe

Abstract

The early years of the internet were marked by a profound optimism about the liberating and democratizing potential of new digital technologies as tools for greater human connection and civic interaction. Yet over the subsequent decades that optimism has curdled into a skepticism - often well-founded - about their impact as the scourges of disinformation, polarization and fragmentation have taken hold on political systems around the world. Meanwhile that same period has revealed the failures of many conventional methods of democracy promotion, including ones using the top-down exercise of hard or soft power. This is what makes democracy-enhancing technologies essential: new applications of cutting-edge digital developments that once more harness these to the cause of open and pluralistic political systems, in manners widely illustrated through the Tech4Democracy Global Entrepreneurship Challenge.

"*Information is the oxygen of the modern age. It seeps through the walls topped with barbed wire. It wafts across the electrified, booby-trapped borders. […] The Goliath of totalitarian control will rapidly be brought down by the David of the microchip.*" - Ronald Reagan, 13 June 1989

"*We must shape the rules that will govern the advance of technologies and the norms of behaviour in cyberspace, artificial intelligence, biotechnology, so they are used to lift people up, not used to pin them down.*" - Joe Biden, 19 February 2021

What Are Democracy-Affirming Technologies?

More separates the above two quotes by US Presidents than time alone. The first was delivered in a speech in London five months before the fall of the Berlin Wall, a time of growing confidence in the march of democratic systems of society and government. President Ronald Reagan's faith in the "David of the microchip" spoke of the prevailing optimism about the role technology would play in that march as the computing revolution took off.

The second quote, made by President Joe Biden to the 2021 Munich Security Conference in the shadow of the January 6 storming of the Capitol, captures democracy's struggles three decades on and the widespread concerns that the flourishing of new technologies in that period have, as the President put it, "pinned people down". The relationship between democracy and technology has proven more conflictual than many hoped and expected at the end of the Cold War.

Yet things do not have to one this way. Technology is not some exogenous force imposed on humanity from on high. From the dawn of time to today it has always been human, and only as good and bad as the humans who created and used it, a truth that applies just as much to cutting-edge Artificial Intelligence (AI) today as it did to the very first stone tools at the dawn of humanity. Our distant ancestors could use their sharpened rocks to exclude, attack and oppress, or to hunt for food, build shelters and protect the community from predators. Likewise, whether the latest technology today harms or serves humanity is up to us.

And so it is with the democracy-technology nexus. As Dr Eric Lander, President Biden's Science Advisor, argued in December 2021: "It's not a guarantee that any given technology will support democratic values. It takes constant vigilance, and constant commitment; we, the people, have to make sure that technology is developed responsibly and used responsibly. That is our solemn obligation."[1] He was speaking at the launch of the International Grand Challenges on Democracy-Affirming Technologies, of which this report is one part.

That solemn obligation is a collective one. It falls to policymakers and politicians, yes, but also to academics and technologists, business people and entrepreneurs, journalists and teachers, campaigners and ordinary citizens. The quest to recognise, promote, and advance "democracy-affirming technologies" belongs to all of us. We all have a responsibility to help reconcile technology and democracy - those formidable twin forces of global human advancement - and bring them back into alignment.

***

This task lies at the heart of the Tech4Democracy Global Entrepreneurship Challenge - one of the International Grand Challenges launched by the White House and State Department in late 2021, and a collaboration with IE University. The Challenge thus provides a rich seam of examples of technology-affirming technologies and how they can drive that reconciliation.

It comprises five continental Venture Days at which a shortlist of start-up and scale-up firms (drawn from hundreds of applicants) have pitched their innovations in fields such as responsible AI and machine learning, fighting misinformation, as well as advancing government transparency and the accessibility of government data and services.

The first Venture Day took place at IE University in Madrid on 28 June 2022, with New Zealand's Prime Minister Jacinda Ardern as keynote speaker. It was won by Citibeats (Spain), which uses ethical big data, natural language processing and machine learning to inform policymaking. Then the Challenge traveled to Bogotá on 10 October, where prizes went to EVoting (Chile), a startup specialising in electronic voting systems, and Matters Lab (USA, Taiwan and Hong Kong), which has developed a Web3 social networking system that substitutes algorithms with human curation. Then it continued to Silicon Valley and Stanford University for the North American stage on 29 November and a keynote address by USAID administrator Samantha Power. Victory there went to Atlos (US), an open-source platform enabling investigators of human rights violations to catalogue and geo-locate eyewitness reports and draw on a community of peers to review them.

As this report goes to press, upcoming Venture Days are scheduled in New Delhi and Cape Town. Then the global final of the Global Entrepreneurship Challenge will take place in Washington DC on March 29-30 alongside the second Summit for Democracy. This will identify a global winner (who will receive a monetary prize and recognition from the US State Department) based on entrants' contribution to democratic values, technological innovation, viability or scalability, and interest for potential investors, as well as the experience, knowledge, skills, and diversity of teams.

Even before that final, the entrants so far have illustrated the range of possibilities for technologies that, in the words of Tarun Chhabra, Senior Director for Technology and National Security on the US National Security Council, "advance the values of privacy, transparency, accountability, and access to information". They are a living, vital rebuke to the fatalistic voices of despair about the relationship between democracy and technology - and a reminder that technology is ours to shape for the good of humanity.

The Current State of Affairs

At the end of the Cold War and the years immediately afterwards, that reality was widely taken for granted. It was a time of Western hubris. Not only had the US prevailed over its Soviet superpower rival, but the liberal democratic model seemed to be spreading around the globe. Central and Eastern European states once under Soviet control were turning to the West. Dictatorships had fallen, or were falling, in regions like Latin America and south-east Asia. Accelerating globalisation promised surging growth and better living standards raising up all, with prosperity strengthening democracy and democracy in turn creating a yet-better environment for innovation and growth. As the American political scientist Francis Fukuyama infamously wrote in 1992, the world appeared to have reached "the end-point of mankind's ideological evolution and the universalisation of Western liberal democracy as the final form of human government"[2].

This confidence was closely bound up with advances in consumer electronics and computing. The writer Evgeny Morozov has recalled how: "Technology, with its unique ability to fuel consumerist zeal - itself seen as a threat to any authoritarian regime - as well as its prowess to awaken and mobilise the masses against their rulers, was thought to be the ultimate liberator"[3]. He even notes that Fukuyama entitled one of the chapter of his book "The Victory of the VCR".

Utopian hopes drove the takeoff of the digital revolution in the 1990s and early 2000s. At a conference in New Mexico in 1996, civic activists, academics and teachers founded the International Association for Community Networking and adopted a series of principles for the internet age like "opposition to media concentration", "support of diverse alternative and marginalised voices", "access to government information", and "commitment to strong democracy"[4]. The former US diplomat Mark Palmer in 2003 set out a plan for ousting the world's 45 remaining dictators by 2025 by harnessing the internet as "a force multiplier for democracies and an expense multiplier for developers"[5]. Such visions rested on the assumption that it would democratise information, lower barriers within societies and provide new spaces for connection, accountability and cooperation that, it seemed, could only strengthen democracy.

Since then technology's sophistication has advanced beyond the wildest dreams of the web-utopians; its exponential growth generally conforming to "Moore's law", the rule of thumb that states that the number of transistors on a dense integrated circuit doubles about every two years. Yet had their optimism been borne out, this would have been accompanied by a similar surge in the global fortunes of democracy. We would all be living in a democratic utopia. If anything, however, the opposite has happened.

The "strongman" style of leadership has taken hold in many major democratic states. Democratic societies are becoming more fractious and divided. The democratic model looks less functional, more fragile, and arguably less appealing. Most indices of global democracy show its rise peaking in the mid-2000s before dropping after the Great Recession of 2008. The American think-tank Freedom House produces an annual report listing the countries where democracy improved over the past year and those where it deteriorated. The last time more countries saw improvements than did deteriorations was 2005. Every year since then the world's countries have been, in aggregate, in democratic decline[6]. Likewise, The Economist Intelligence Unit's Democracy Index fell in 2021 to the lowest level since its inception in 2006.[7]

***

Part of the explanation is geopolitical. Among the economies that have risen most since the Great Recession are a number of non-democracies, most notably China. It has thus come to represent an alternative model of state and society for other states, particularly in the developing world, and in certain cases (Myanmar, Venezuela, Angola) a sponsor of other autocracies.

The greatest geopolitical ally to authoritarianism has been not Chinese power, however, but the growing power of instability and chaos in a "G-Zero world" (to borrow a phrase from the American political scientist Ian Bremmer) in which no one country or even group of countries can establish order. Examples like Russia's attacks on Georgia and Ukraine, Iran's sponsorship of foreign militias, the atrocities of the Syrian, Yemeni, and Tigray wars, and the persecution of the Rohingya in Bangladesh all illustrate this "Age of Impunity" (that term coined by David Miliband, President of the International Rescue Committee[8]) and how it is innately damaging to the often-fragile democracies of the countries concerned.

Yet important though such factors have been, many of the threats to democracy originate within democratic societies themselves. Democracy is not just about casting one's ballot in an election. It is also a dense eco-system of institutions and practices. Power must be contained by checks and balances, the rule of law, and norms concerning its use. Information must be free and debates pluralistic. The Harvard political scientists Steven Levitsky and Daniel Ziblatt argue[9] that the two most fundamental pillars of democracy are mutual toleration ("the understanding that competing parties accept one another as legitimate rivals") and forbearance ("the idea that politicians should exercise restraint in deploying their institutional prerogatives"). This eco-system of institutions and practices has been weakened in recent years.

In America, for example, politics has become unhealthily polarised. Polling by Pew Research[10] charted the shift between 1994 and 2014. Where at the start of that period there was substantial ideological overlap between Democrats and Republicans, by the end of it 92% of Republicans were to the right of the median Democrat, and 94% of Democrats were to the left of the median Republican. Partisanship had intensified into mutual demonisation: 36% of Republicans saw the Democratic Party as a threat to the nation's well-being by 2014 (up from 17% two decades before) and 27% of Democrats felt that way about the Republican Party (up from 16%). The gap has widened significantly beyond 2014, to the point where today some two-thirds of Republican voters do not recognise President Biden's legitimate election in 2020.[11]

Prominent though the fractures in US democracy are, they are far from unique. From India to Brazil, the Philippines to Poland, democracies are not failing suddenly but being eroded gradually under what the political scientists Aziz Huq and Tom Ginsburg have called "constitutional regression"[12]. A study of over 4.8 million respondents in 160 countries by the Centre on the Future of Democracy at Cambridge University found that "across the globe, younger generations have become steadily more dissatisfied with democracy - not only in absolute terms, but also relative to older cohorts at comparable stages of life."[13]

***

One major explanation for these shifts is that the globalisation unleashed around the end of the Cold War has lifted living standards in much of the world but has disproportionately benefited those at the top, producing a degree of economic polarisation (and often spatial polarisation: the elite lives apart from the rest) that is dangerous to democracy. Another explanation is that collective institutions from religions bodies, political parties and trade unions to clubs, societies and mass newspaper readership have given way, to greater and lesser degrees, to fragmentation and individualism. Some elements of this are positive, implying greater personal freedoms and choice. But it also heightens the risk of polarisation, declining mutual trust, and culture wars that collectively put the toleration and mutual forbearance at the heart of democracy at risk.

Nonetheless, technology is arguably a more fundamental explanation than either economic or social polarisation. For one thing, it is a root cause of both. At the top of the income scale the internet revolution has increased the income premium associated with high levels of education; at the bottom of the income scale it has meant the automation of many manual and less-skilled jobs. And the internet revolution has also driven the shift to a more fragmented and individualistic society. If communal spaces are in decline, be they cafés or clubhouses or sites of worship, that is in no small part due to the switch from offline interactions and pastimes to online ones.

That might not be so detrimental to democracy if, as the techno-optimists had hoped, new online communal spaces enabled civil encounters with a range of fellow citizens. All too-often, however, the shift online has arrayed citizens into echo chambers of like-minded opinion and pushed them farther from the compromising and open-minded spirit of a robust democracy towards ever-more intractable attitudes. Algorithms designed to maximise engagement drive users towards more and more extreme content to maintain their attention: one study of 72 million comments on about two million online videos between May and July 2019 found users routinely migrating from milder "alt-lite" content towards more hardline "alt-right" content.[14]

Another, related form of polarisation concerns facts themselves, without a commonly accepted basis for which constructive democratic debate is impossible. Speaking at the Venture Day in Madrid, Prime Minister Ardern (citing former German chancellor Angela Merkel) noted that where once people would see something on the nightly TV news and discuss it around the water cooler at work the next day, now they get their news online and the water cooler discussion concerns whether it is real or not. "If people are fiercely of the view that fiction is fact or fact is fiction, it is incredibly hard as leaders to build consensus in that environment," she said. The Covid-19 pandemic brought alarming new illustrations of how quickly disinformation can now spread online, as myths and conspiracy theories about safe vaccines rippled around the world and undermined public health efforts.[15]

The technological explanation for democratic decline also concerns the quote at the start of this chapter. President Reagan's assertion that the "David of the microchip" would defeat the "Goliath of totalitarian control" has in places proven correct (consider how social media has sustained the ongoing protests in Iran even in the absence of a leader or figurehead). But at least as often, and arguably more often, Goliath has been able to co-opt David for his own purposes. "Digital technology has also reinforced rather than undermined the hold on power of many non-democratic regimes", wrote the political scientist David Runciman in 2018, citing such examples as Ethiopia and Venezuela: "Far from being a decisive weapon in the hands of freedom fighters, it has become an essential tool for keeping tracks on them."[16]

***

What, then, is to be done? Unfortunately, major international examples of how *not* to defend and advance democracy are more abundant than those of how to do so successfully. One product of the "end of history" hubris of the end of the Cold War was the belief that hard power could be used to topple tyranny and thus create the room for democracy to emerge. Such thinking was discredited by the wars in Afghanistan and Iraq, and although the West's support for Ukraine in defending itself against Russia's full-scale invasion does show the place for hard power in defending democracy, a crucial distinction there is that Kyiv's allies are supporting a sovereign democratic government rather than seeking to summon up democratic spirits in states where they do not yet command legitimacy.

An alternative to hard-power democracy promotion is of course the use of soft-power; funding political education initiatives and free media outlets, training election officials and supporting initiatives to boost participation. But the effectiveness of this approach is open to question. The Yale University political scientist Sarah Bush has written[17] of research in Jordan in 2012, during which she attended a training workshop for the country's weak political parties run by an international NGO worker named Rana. "On the day of the workshop, several men showed up that were not on Rana's participation list. The men sat quietly throughout the workshop, taking notes and observing… [T]he other participants became uncomfortable." The men were from the Mukhabarat, Jordan’s omnipresent intelligence agency. Bush’s anecdote illustrates the limits of attempting to seed democratic norms from above in systems otherwise at odds with them.

Another mistake is treating the supporters of authoritarian politicians or causes as the enemy. In a world in which democracy can feel ever-more embattled, and where the forces of authoritarianism often seem to reinforce each other, this them-and-us mindset is understandable. But it is usually not a constructive foundation for the mutual toleration and forbearance that a resilient democracy requires. As the journalist Anand Giridharadas recently put it[18], the pro-democracy movement needs to meet people where they are. He advocates “more space in movements for people who don’t fully get it, who don’t use the right terms, but their hearts are in the right place [and] are suspicious or nervous about some of the ideas they hear from portions of the pro-democracy side”. The problem, he adds, is that: “We’re often more interested as a movement in policing their entry, rather than saying, ‘Come on in.’”

These examples of what not to do provide framework for future efforts at promoting democracy: the focus should be on using soft power within societies rather than hard power over whole societies, on bottom-up methods of encouraging democracy rather than top-down impositions, and on the underestimated art of persuasion rather than a them-and-us approach. All of which makes a compelling case for democracy-enhancing technologies, which meet each one of these points. Today’s technologies set the framework for societal and individual behaviour. They codify the norms and standards of civic life. They are the arena in which persuasion takes place. And that is without getting into the realm of tomorrow’s technologies; of how developments like genuinely humanlike AI and robotics, lifelike virtual reality in the metaverse, and brain-computer interfaces will intensify all of these.

It is remarkable that the notion of democracy-enhancing technologies has until recently remained so under-explored where other less effective methods of democracy promotion have been allowed to consume such resources. Now is surely the moment to make up for lost time.

Perspectives for the Future

The pace of global democracy’s deterioration in recent years, and challenges arrayed against it, can make for a daunting outlook. But there are grounds for optimism. The year 2022 was in many respects a good year for the cause. Russia’s full-scale invasion of Ukraine elicited a resilience from the Ukrainian people, in defence of their democratic sovereignty, that Vladimir Putin and others clearly had not anticipated. It also prompted the US and its allies to pull together and support Ukraine in its fight, again to a greater degree than might have been expected. Democracies around the world have defied the gloomier predictions about the impact of knock-on shocks to energy and other prices. One does not need to subscribe to the “End of History” hubris of the early 1990s to see how all this contradicts the fatalistic narrative of democracies hopelessly divided and unresponsive in the face of the authoritarian challenge.

On multiple fronts the strongman model has showed its weaknesses lately. Russia’s military failures in Ukraine were clearly a product of poorly motivated troops and lacking accountability in the Kremlin. China’s authoritarian system proved its failings as the government’s dogmatic Zero Covid strategy failed and crumbled. Those failures have set back the country’s economic rise and tarnished its model in the eyes of the world. In Turkey, over-centralised leadership and the ensuing ill-judged monetary policies have led to economic instability that could conceivably see a change of president later this year.

The reverse side of these failures is an argument about the enduring strengths of the democratic model. When it works as it should, it allows talents to rise, holds the powerful accountable, and ejects them when they are no longer effective or wanted. It ensures multiple perspectives are heeded in collective decision-making. It can correct its course. Internationally it amounts to collaboration based not just on raw interests, but values too. When they work like that, democracies can be cohesive at home and responsible global citizens abroad.

In those truths lie the makings of a strategy for democratic fightback, one built on foundation of confidence in the democratic system and ideal, in societies that are open, pluralistic, and collaborative. Such a fightback means better access to information, more (and more civil) encounters between different points of view, open and responsive government, stronger individual rights, a culture of both enlightened scepticism and mutual respect, and one of mutual toleration and forbearance that always leaves room for the possibility that one is wrong and one's opponent is right. It means encouraging structures that reduce barriers and enable people to congregate, exchange and ideally reach and execute informed decisions as a society. A healthy democracy is a river, fluid and dynamic and constantly refreshed with new nutrients, not a stagnant pond.

The Global Entrepreneurship Challenge has modelled the sorts of technologies, and technological applications, that support this strategy - and provided a reminder that the verve and originality out there is up to the scale of the task, if only it can be harnessed. It shows that democracy-enhancing technologies can and must be at the heart of the democratic fightback, creating a digital eco-system that is friendly to democracy not because it has been imposed from above but because it has grown up organically through the choices and habits of citizens, and encouraged the better angels of human nature to prevail. All technology is human. Democracy-enhancing technology makes a virtue of that.

Conclusion

The alienation of technology from the cause of democracy is not inevitable: technology has always been a human construct, its moral quality a function of the humans who create and use it. Nor is the "democratic recession" of the past years inevitable. The past year especially has shown that while democracies can have their weaknesses, autocracies - with their concentrations of power and poor ability to course-correct - have significant vulnerabilities too. These twin realities should ward us off fatalism. Things can be fixed. Democracy-enhancing technologies, drawing on the broadest possible scope of human agency and originality, can be a major part of the solution in reconciling once more those twin forces of human forces and turning the tide on illiberalism and authoritarianism.

Endnotes

1 The White House. (2021, December 8). White House announces launch of the International Grand Challenges on Democracy-Affirming Technologies for the Summit for Democracy. https://www.whitehouse.gov/ostp/news-updates/2021/12/08/white-house-announces-launch-of-the-international-grand-challenges-on-democracy-affirming-technologies-for-the-summit-for-democracy/

2 Fukuyama, F. (1992). The End of History and the Last Man. Hamish Hamilton.

3 Morozov, E. (2012). The Net Delusion: How Not to Liberate The World. Penguin.

4 International Association for Community Networking. (n.d.). http://www.partnerships.org.uk/iacn/IACN.html

5 Palmer, M. (2003). Breaking The Real Axis of Evil: How to Oust the World's Last Dictators by 2025. Rowman & Littlefield.

6 Freedom House. (2022). Freedom in the World 2022. https://freedomhouse.org/sites/default/files/2022-02/FIW_2022_PDF_Booklet_Digital_Final_Web.pdf

6 The Economist. (2022, February 9). A new low for global democracy. https://www.economist.com/graphic-detail/2022/02/09/a-new-low-for-global-democracy

7 International Rescue Committee. (n.d.). Welcome to the age of impunity: David Miliband's World Economic Forum speech. https://www.rescue.org/press-release/welcome-age-impunity-david-milibands-world-economic-forum-speech

8 Levitsky, S., & Ziblatt, D. (2018). How Democracies Die. Crown.

9 Pew Research Center. (2014, June 12). Political polarization in the American public. https://www.pewresearch.org/politics/2014/06/12/political-polarization-in-the-american-public/

10 NBC News. (n.d.). Anger in minds: NBC News poll finds sky-high interest, polarization ahead. https://www.nbcnews.com/meet-the-press/first-read/anger-minds-nbc-news-poll-finds-sky-high-interest-polarization-ahead-m-rcna53512

11 Huq, A., & Ginsburg, T. (2018). How to Lose a Constitutional Democracy. Chicago Unbound, University of Chicago Law School.

12 University of Cambridge. (n.d.). Youth and satisfaction with democracy. https://www.cam.ac.uk/system/files/youth_and_satisfaction_with_democracy.pdf

13 MIT Technology Review. (2020, January 29). A study of YouTube comments shows how it's turning people onto the alt-right. https://www.technologyreview.com/2020/01/29/276000/a-study-of-youtube-comments-shows-how-its-turning-people-onto-the-alt-right/

[14] Johnson, N. F., et al. (2020). The online competition between Pro- and Anti-Vaccination Views. Nature, 582.

[15] Runciman, D. (2018). How Democracy Ends. Basic Books.

[16] Bush, S. S. (2015). The Taming of Democracy Assistance. Cambridge University Press.

[17] Harvard Gazette. (2022, October). How to protect democracy: Don’t give up on your neighbor. https://news.harvard.edu/gazette/story/2022/10/how-to-protect-democracy-dont-give-up-on-your-neighbor/

2. Mapping Democracy-Affirming Technologies Worldwide. Darío García de Viedma & Alejandro Roche

Abstract

Democracy-affirming technologies hold immense potential for bolstering democratic values and processes, but these technologies may not prioritize democratic values by design. This paper addresses the misalignment between the democratic use cases of Tech4Democracy startups and the actual design of their technologies and explores the implications for democratic values and participation. Drawing on a methodology that combines a Tech Radar approach and NLP analysis of a worldwide patents database, this analysis investigates the current landscape of democracy-affirming technologies based on a Global Entrepreneurship Challenge organized by IE University (Center for the Governance of Change & Center for Entrepreneurship and Innovation) in partnership with the U.S. Department of State and with the strategic support of Microsoft. The analysis reveals such risks associated with the lack of democratic intentionality in technology design as unexpected biases, exclusionary practices, and public distrust.

Introduction

"Ethics by Design" is an approach advocated by the European Commission to address ethical issues in AI development. It emphasizes the proactive integration of ethical principles as system requirements during the development stage. The goal is to prevent ethical issues from arising in the first place rather than attempting to fix them after the system's deployment. This “Ethics by Design” framework nevertheless recognizes that some ethical concerns may only become apparent during development and others post-deployment. The principles are used as guidelines to steer the design process, and ethical requirements may extend to not only the AI system, but also the development processes.[1]

A similar logic could be applied to democracy-affirming technologies. Just as "Ethics by Design" seeks to embed ethical considerations into AI systems, democracy-affirming technologies can be democratic by design. In other words, principles and requirements that support democratic values and processes should be incorporated into the development of these technologies. By incorporating democratic values like transparency, citizen engagement, and inclusivity into the core system requirements, we improve the potential to preemptively address or lessen democratic challenges that may surface during the implementation or utilization of these technologies.

In this report, we explore the conceptual contrast between two distinct areas of technology as it intersects with democratic systems: "tech for democracy" and "democracy-affirming technologies".

On the one hand, "tech for democracy" here refers to technology products that are applied to democracy-related use cases, e.g., digital tools for organizing political campaigns, platforms for civic engagement, and systems for online voting. On the other hand, "democracy-affirming technologies" is a term defined by Blázquez-Navarro in the foreword of this report. These technologies are designed, developed, and deployed with a specific purpose in mind: to foster core democratic values, principles, and rights throughout their lifespan. Among the core values, principles, and rights that these technologies aim to support are personal liberty and autonomy, privacy, data protection, inclusion, access to truthful information, the promotion of critical thinking around technology, the enablement of technologically savvy legislative bodies, the participation in free elections, the separation of powers, the principle of legality, and the rule of law.

Our objective in this report is to use an international sample from the startup ecosystem to show how this sector is using existing technologies to build applications that support democracy. Our research reveals that there is no deliberate effort to create democracy-affirming technologies per se, and this observation prompts us to consider a wide range of interpretations about the potential risks and opportunities that come with the ongoing development and establishment of democracy-affirming technologies.

Methodology

Sampling: A worldwide startup competition

IE University hosted tech startups competitions in five continents: Europe (at IE University in Madrid), South America (at Universidad de los Andes in Bogotá), North America (at Stanford University in Silicon Valley), Asia-Pacific (with ORF in conjunction with the Raisina Dialogue during the G20 in New Delhi), and Africa (at the University of Cape Town). The five continental winners competed in a Global Final in Washington, D.C.

More than 300 startups from 68 countries applied to be part of one of the six competitions of Tech4Democracy's Global Entrepreneurship Challenge. Indeed, startups all around the world were contacted by IE University's Center for Entrepreneurship and Innovation, either directly or through databases, associations, and networks, to inform them about the open calls and encourage them to apply.

For every one of the six challenges, an online semifinal was held for between 9 and 11 selected organizations to select between three and six finalists for each in-person event.

At both the semifinals and the finals, each competitor had five minutes to pitch their solution, and then a panel of judges had five additional minutes to ask questions of each competitor.

The evaluation criteria for both the semifinal and the final (below) were all weighted equally:

- Contribution to democracy: To what extent does the organization's technological solution have the potential to contribute to the defense and promotion of liberal democracy as a political system and of democratic values such as liberty, equity, inclusion, privacy, freedom of expression, access to information, transparency or fairness?

- Technological innovation: To what extent does the organization's solution leverage digital or other technologies that are relatively new/uncommon or are used in relatively new/uncommon ways?

- Viability/scalability: To what extent is the organization's technological solution commercially viable (if it is still in its development phase) or scalable (if it has already been commercialized)?

- Interest for investors: To what extent is the organization's technological solution interesting for investors due to its potential profitability?

- Team: To what extent does the organization count with an excellent leadership team and staff? Taking into account experience, knowledge, skills, and diversity.

This study uses a sample of 53 semifinalist startups to extrapolate about the current landscape of technology-affirming startups, with a focus on their origin, area of focus, the gender of the founder, and the maturity of their technology.

We acknowledge that this methodological approach presents certain limitations. It does not necessarily represent the entire sector but rather those who self-selected by participating in Tech4Democracy and were subsequently chosen as semifinalists. What is more, the 53 semifinalists were selected by IE University within a startup competition that the same institution organized., so the sample is biased toward the scope of our outreach and our selection criteria. The process of categorization is inevitably somewhat artificial.

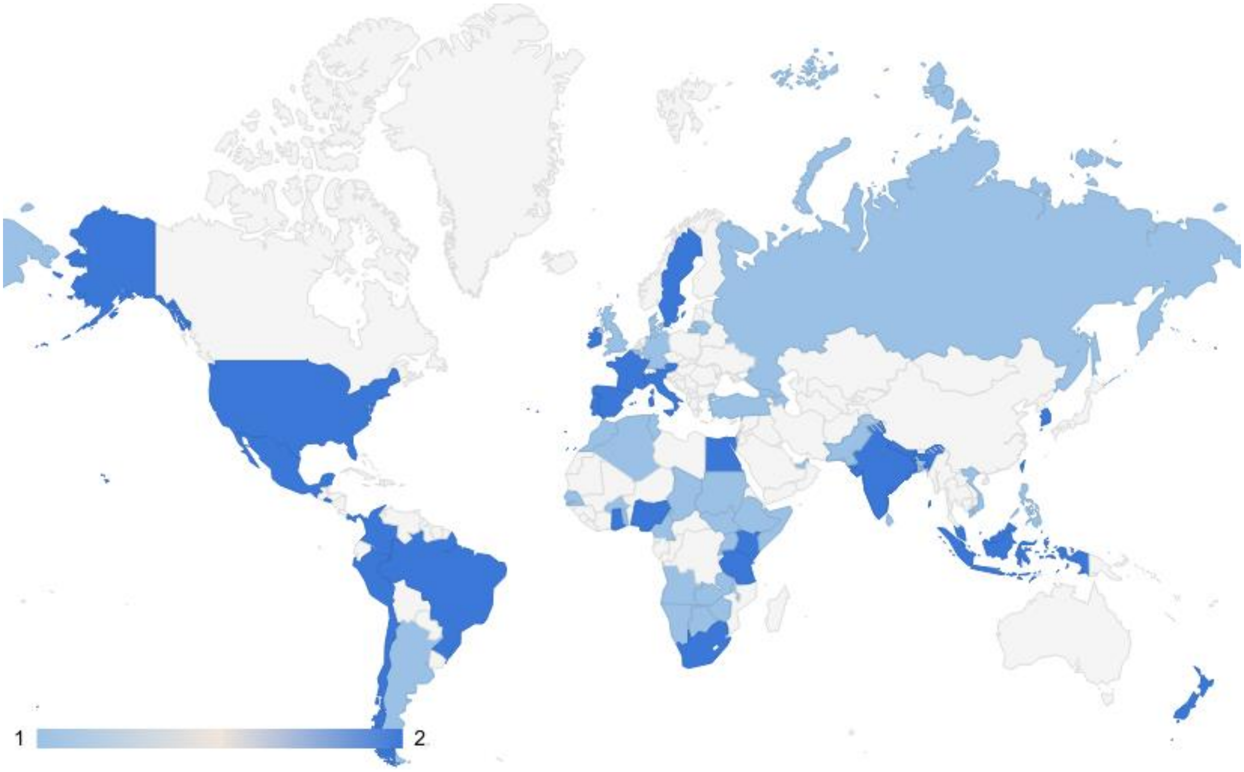
We aimed to develop a methodology that would be both appropriate and innovative for our purposes informed by these limitations imposed by the sample size, data availability, and the rapidly changing landscape of the intersection of society and technology,. This investigation did not yield a comprehensive body of scientific evidence, but it illuminates potential opportunities and insights for industry stakeholders to further enhance the democratic implications of their technological applications.

This initial venture into uncharted territory seeks to be groundbreaking in terms of not only content and its visibility within the confluence of society and technology, but also methodology. Despite the acknowledged constraints, we have striven to pioneer a methodology that balances rigor with the necessity for swift understanding in a fast-paced and evolving field. The preliminary outcomes from this effort underline the importance of continuing this line of inquiry.

Worldwide distribution of participants

300 organizations from 68 countries applied to compete in the Global Entrepreneurship Challenge. 53 semifinalists were selected from that sample, representing 29 countries.

Map 1: Countries represented in the Global Entrepreneurship Challenge. Dark blue indicates startups that reached the semifinal, whereas light blue indicates countries where the startups that competed did not reach the semifinal.



Distribution by area of focus

Our Global Entrepreneurship Challenge **identified ten areas of innovation where democracy-affirming tech organizations are making an impact.** The areas, listed from the most to the least represented in our sample, are:

- CivTech (12 startups): Digital platforms that leverage technology to facilitate, promote, and enhance citizen engagement in policymaking (through expressing opinions, voting on alternatives, proposing solutions, etc.) and/or connection, interaction, and collaboration between citizens and policymakers.

- Equity and inclusion (9 startups): Organizations that use technology to defend and promote social equity and inclusion of women, economically disadvantaged groups, people with disabilities, and underprivileged groups in general.

- Enhanced social networking (8 startups): Digital platforms that allow for a better social networking experience by decentralizing control of the network through web3 technologies or introducing moderation and other tools to foster a healthier civic conversation and combat polarization, fake news, and hate speech.

- Data for policymaking (6 startups): Technologies that deliver better data collection, processing, and visualization to inform policy- and decision-making processes in a way that is respectful of privacy and individual rights.

- Digital identity and trust (5 startups): Transparency technologies and identity recognition or protection technologies that ensure inclusive access to digital public services and protection of sensible data.

- Tools to fight disinformation (3 startups): Technologies that support fact-checking efforts, identify bot activity, or work on social data to promote accurate information on key matters, including electoral processes.

- GovTech (3 startups): Organizations that apply digital technologies to improve, modernize, and optimize government services, operations, and administration–notably with a focus on public procurement processes.

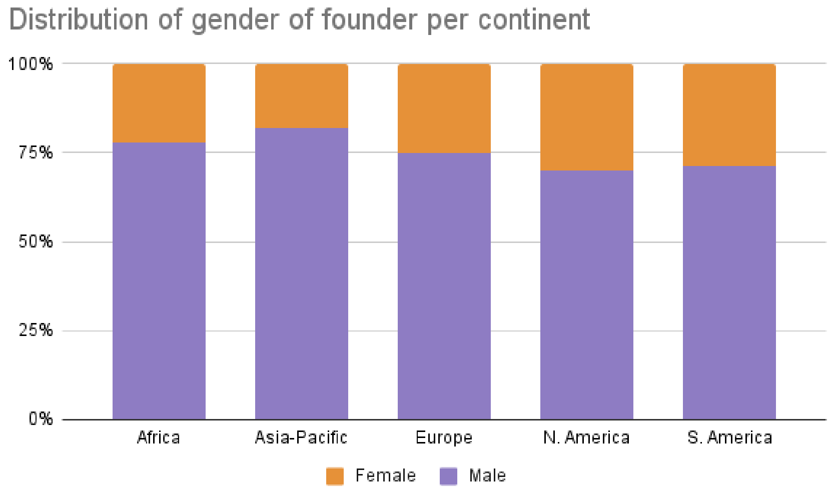
- E-voting (3 startups): Startups that allow for the organization of secure digital electoral processes, often through the use of encryption, and facilitate voting.

- Campaigning (3 startups): Digital solutions to organize large campaigns (either political campaigns for public office and/or campaigns for social change) with tools that facilitate public outreach, supporters' engagement, data management data, etc.

- Responsible AI (1 startup): Automated decision-making systems that provide equal opportunity, do not discriminate and are fair, explainable, auditable, ethical, and accurate.

Distribution by gender of founder

The gender distribution among startup founders varies significantly across different regions. The gender distribution is the most balanced among the North American participants, with 70% of startup founders being male and 30% female. This region is leading the way in gender parity among startup founders. In contrast, the Asia-Pacific region has the least gender balance, with 82% of startup founders being male and only 18% female.



This disparity highlights the need for more initiatives to support and encourage female entrepreneurship in the Asia-Pacific region. This inequality is reflected compare these figures with global data. According to the Global Entrepreneurship Monitor (GEM) 2021/2022 report, startup rates for women dropped by 15% from 2019 to 2020.[2] Another study indicates that men still outnumber women 3-1 among business owners.[3]

Building a tech radar through an NLP analysis of a patent database

A tech radar visualizes the varying applications and maturity levels of different technologies. Our aim was to ascertain which types of technologies are being employed in the four major areas of innovation boasting the highest volume of startups: civtech, enhanced social networking, data for policymaking, and equity and inclusion. We selected 16 technologies or interfaces extensively used in the industry: Analytics, Augmented Reality (AR), Big data or LLM integration, Biometrics, Chatbot, Cloud, Cybersecurity, Distributed Ledger Technology (blockchain, cryptography), Machine Learning, Natural Language Processing (NLP), Open-Source Software, Predictive Analytics, Quantum computing, Social Media interface, Virtual Reality (VR), and Web or mobile interface.

Our research methodology was built around a systematic Boolean query search of the World Intellectual Property Organization (WIPO) database, a data set selected for its comprehensiveness, inclusivity of worldwide patents, and its integrated translation functionality. WIPO's database, PATENTSCOPE, ensures immediate access to published International PCT applications in full-text on the day of publication.[4]

A unique query was formulated for each of the 16 technologies that used Boolean operators to include all patents meeting the specified criteria and exclude those unrelated to the technology under scrutiny. WIPO's automatic translation tool, WIPO Translate, enabled the inclusion of patents filed in languages other than English and supported a thorough, global overview of the patent landscape for each technology.

Technology maturity can be quantified in many ways (e.g., market size, investment, momentum in conversations), and we chose to classify technologies based on the number of global patents. The reasons for this classification were two-fold: (a) it enabled a systematic methodology applicable to all technology branches; and (b) measuring the number of patents curbed the bubble effect, which could inflate results if other values (e.g., capital or user base) were measured.

A potential risk of using patent count as a proxy would be a tautological fallacy: technologies that rely on Open-Source code would not be considered as mature as they actually are because, by nature, they have fewer patents. Another potential limitation of this approach would be overlooking actual usage in regions with diverse intellectual property regimes or in rapidly advancing sectors like artificial intelligence and quantum computing.

To augment the robustness of our methodology, we recommend that future research integrates such additional metrics as market size, investment volume, momentum in academic and industry discourse, user base size, and sentiment analysis. Moreover, we propose a shift from an exclusive focus on absolute volumes to an analysis of trends to provide critical insights into the technologies that are gaining momentum.

We found some technologies with a much higher number of patents: social media interface (6,001,553), web or mobile interface (2,817,524), and predictive analytics (2,222,429). The technology branches with markedly fewer patents were natural language processing (16,336), conversational AI (29,503), and quantum computing (40,101).

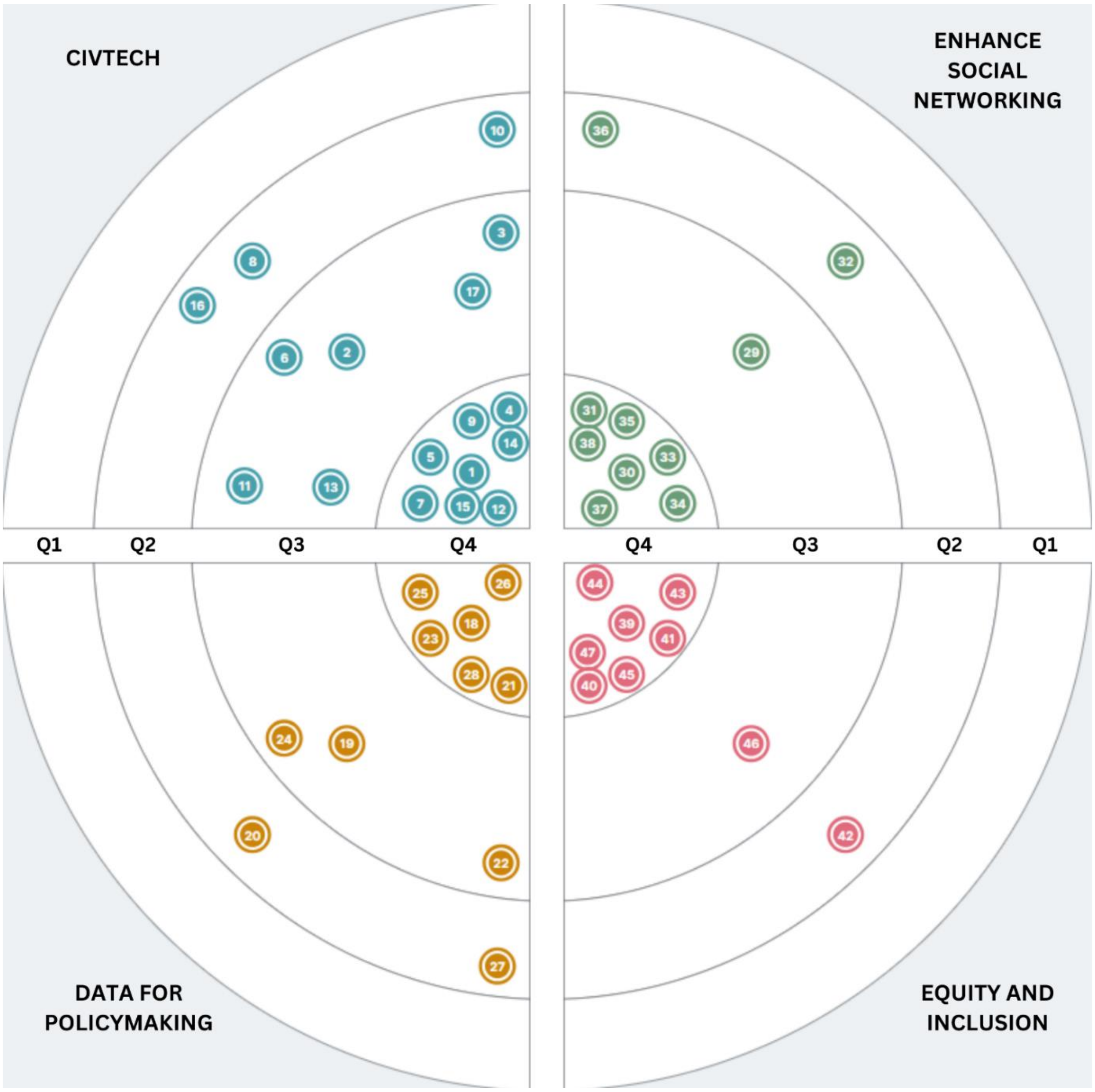
We used the interquartile range (IQR) method to define quartiles for the patent count data, calculating the range between the 25th and 75th percentiles of the sorted data. The patent counts at the 25th, 50th, and 75th percentiles determined the ranges for Q1 (between the 3rd and 4th patent counts, approx. 2,079,967), Q2 (between the 8th and 9th patent counts, approx. 711,112), and Q3 (between the 12th and 13th patent counts, approx. 264,976).

Finally, we classified the participating startups not only by their area of innovation but also by the technologies they employ. Some utilize several. Each technological application of a startup represents a data point, or what ThoughtWorks, the consultancy that devised the tech radar, call a "blip". We modified the quadrant and ring terminologies utilized in the ThoughtWorks template to better fit our working framework.

Results

A visual inspection of the constructed tech radar makes clear that none of the companies included in this study are implementing technologies from the first interquartile range with the least number of patents, namely natural language processing (16,336 patents), chatbot (29,503 patents), quantum computing (40,101 patents), and distributed ledger (156,013 patents). The heart of the radar is densely populated with technologies exhibiting a high volume of patents. The most adopted technologies among the surveyed companies include social media interface with a staggering 6,001,553 patents, followed by web or mobile interface (2,817,524 patents), predictive analytics (2,222,429 patents), and augmented reality (1,937,504 patents).

Tech Radar: Each quadrant represents one of the four most common areas of innovation within the Tech4Democracy Challenge. Each blip represents the technologies used by those companies. The rings represent the interquartile intervals: Q1 comprises the technologies with least patents and Q4 the technologies with most patents.



Discussion

The results derived from the technological radar suggest that the companies within our sample are utilizing mature technologies and customizing them for the democracy-related industry. They seem to be building their value proposition on the creation of web or mobile interfaces that are user-friendly for various buyer/user personas within this sector (e.g., public institutions, citizens or officials). These entities also appear to be developing business models tailored to meet the consumption requirements of their respective clientele. For a comprehensive comparative analysis, an analogous tech radar assessment across various technology sectors is essential. This approach will enable us to ascertain whether the adoption rate of mature technologies in the field of democracy-affirming technology is above or below the average. For example, the adoption of machine learning is on the rise in fintech. Nearly 90% of companies anticipate an increase in their utilization of machine learning in the forthcoming 12 months, with a significant 45% forecasting a substantial surge.[5]

What are the risks associated with these results?

A misalignment can arise between the goals of commercial technologies and those of democracy-affirming technologies. This misalignment is exacerbated when Tech4Democracy startups repurpose commercial technologies for democratic use cases. The implications of this misalignment could be significant, particularly in terms of inclusion and engagement.

Inclusion is a critical aspect to consider when designing software for the democracy sector. Moyo (2022) discusses long-standing quality practices in software development, including the importance of designing high-quality software development methods that promote inclusion.[6] This approach is consistent with the need to consider all different use cases and potential excluded groups when designing software for the democracy sector. For instance, when designing a voting app, developers should consider the needs of various user groups, including those with disabilities. This could mean incorporating features like text-to-speech for visually impaired users or simplified user interfaces for elderly users who may not be as tech-savvy.

Something that bureaucracy and coding have in common are protocols. If protocols are designed to support diversity, then the result of the protocol will be inclusive toward the diverse group. For example, a protocol in a government service portal could be designed to provide information in multiple languages, thereby ensuring that non-native speakers are not excluded from access to important services. It is, however, important to note that bias is unavoidable in software design. The creator of the model chooses the criteria for inclusion when conceptualizing, building, and training it. A user may not even be aware of the bias generated and the criteria to fix it that exist.

To underscore the significance of this limitation, let us revisit the earlier example of a voting app designed with inclusivity in mind. Despite the developers' meticulous efforts to make the app accessible for visually impaired users, they may inadvertently overlook certain types of visual impairments. This could result in a product that, while inclusive for some, still exclude others. Tiago Guerreiro's PhD thesis provides a compelling exploration of this issue. Guerreiro conducted a comparative study of how individuals with varying degrees of sight interact with the same app. His findings revealed substantial differences in usability experiences among the participants and underscored the complexity of designing truly inclusive technology UX/UI.[7] This highlights the need for comprehensive protocols in technology design that ensure that all potential user groups are considered during the development process and minimize the risk of unintentional exclusion. Within this same report, Trisha Ray further develops this idea.

Toussaint et al. (2022) discuss the propagation of bias through design choices in on-device machine learning workflows for AI/ML models. They highlight that design choices during model training, like the sample rate and input feature type, and optimization, like light-weight architectures, the pruning learning rate, and pruning sparsity, can result in disparate predictive performance across different groups.[8] This underscores the importance of being aware of potential biases and taking steps to mitigate them in the design process. This is not possible when adopting external models.

Social network models have gained traction in the Tech4Democracy sector, where they are being applied to enhance communication between citizens and between citizens and their governments. Many cities and citizen collectives are implementing social network models, however, social networks thrive on the engagement economy and assign criteria to their information sorting algorithms to privilege content that can generate more engagement and clicks.[9] Potential deployers of these citizen social networks must question the trade-off: implement their processes of citizen "social networking" on existing platforms and take advantage of their network effect (more users lead to more users), or opt for the creation of unique social network platforms using algorithms that may be more democracy-oriented by design.

The tech radar discussed here presents a series of questions that surpass available answers. Two primary inquiries arise: why does this situation occur, and how can it be enhanced?

The question of market size is particularly pertinent. The development of such transformative technologies as generative AI, blockchain, quantum computing, and conversational AI is often constrained by significant costs and risk factors. The market for these technologies, particularly within the context of democracy-affirming applications, might not be sufficiently mature or expansive to attract enough funding and resources to stimulate and expedite development. Without adequate financial incentives, the evolution and integration of these technologies within the democratic framework may be hindered.

Regulation, particularly in the realm of sensitive data handling, is a crucial balancing act. While these frameworks aim to protect individual rights and uphold ethical standards, they can inadvertently constrain technological innovation. For example, strict data protection regulations, as necessary as they are, may limit the full utilization of AI in areas like opinion analysis and predictive policymaking. This observation is not a critique of regulation, but a call for its evolution and foster a dialogue that results in adaptive regulations that not only respect privacy and individual rights, but also enable technological progress. This balance will require active engagement from all stakeholders, including policymakers, technologists, and society at large. Through collective effort, we can cultivate an environment where both democratic values and technological innovation can thrive.

Conclusion

Democracy-affirming technologies might not be democratic by design. The data obtained from the Tech4Democracy startup competition highlights the risks and challenges faced in creating democracy-affirming technologies. Biases, exclusions, and the erosion of public trust are among the primary concerns when democratic intentionality is overlooked.

To address these issues and promote the democratization of AI, a multi-faceted approach is required. Collaborative efforts between policymakers, technologists, and researchers are essential to embed democratic principles into technology design processes. By mapping AI development and focusing on areas where democratic technologies are most needed, we can foster inclusive and participatory governance, civic engagement, and social justice.

Continued research is crucial to further explore innovative strategies that align technology with democratic values. By actively monitoring AI projects and infusing democratic principles at their core, we can create a future where technology empowers citizens and promotes social equity.

Endnotes:

[1] European Commission. (2021). Ethics By Design and Ethics of Use Approaches for Artificial Intelligence

[2] Global Entrepreneurship Monitor. (n.d.). Women's entrepreneurship, https://www.gemconsortium.org/reports/womens-entrepreneurship

[3] World Economic Forum. (2022). How Women Entrepreneurs Are Narrowing The Venture Capital Gender Gap, https://www.weforum.org/agenda/2022/07/women-entrepreneurs-gusto-gender

[4] https://patentscope.wipo.int/search/en/search.jsf

[5] Netguru. (2023). The State of Machine Learning in Fintech, https://www.netguru.com/machine-learning-in-fintech-report

[6] Moyo, S. (2022). Some Long-Standing Quality Practices in Software Development, http://arxiv.org/abs/2209.08348v1

[7] Guerreiro, T. (2014). User-Sensitive Mobile Interfaces: Accounting for Individual Differences amongst the Blind. ArXiv, https://arxiv.org/abs/1402.1036

[8] Toussaint, W., Ding, A. Y., Kawsar, F., & Mathur, A. (2022). Tiny, always-on and fragile: Bias propagation through design choices in on-device machine learning workflows, http://arxiv.org/abs/2201.07677v4

[9] Ozesmi, U. (2019). The Prosumer Economy -- Being Like a Forest, https://arxiv.org/ftp/arxiv/papers/1903/1903.07615.pdf

GEOPOLITICS, GOVERNANCE AND DIPLOMACY OF TECHNOLOGY: RECENT TRENDS

3. Tech Diplomacy and Tech Governance.

Cathryn Clüver Ashbrook

Abstract

With technology becoming the frontline of geopolitical competition and control, this chapter explores the emerging discussion on the shape of technological governance in the context of an accelerating rivalry between democracies and autocracies. With restrictions on access to technology rising and regulations implemented that reflect starkly different appreciations of technology's use in society and a "renationalization" occurring in the West and in China, where even open-source code is actively being replaced by national solutions in a desire for sovereignty, the "Balkanization" of digital ecosystems is occurring. The Western response has been at once to increase bilateral and minilateral cooperation, which might lead to the creation of a "democracy-led" digital tech and regulatory space, providing existing barriers are addressed. This chapter briefly surveys the existing landscape and examines the possibility and pitfalls of creating a wider, democracy-led T-12/T-14 alliance structure as a coordination and governance model of the near-term future in technology policy terms. It concludes that instead of a linear march toward a wider governance structure, a patchwork of deepening and coordinating nodes on tech governance by and for democracies is more likely in the short-term, to facilitate practical alignment. Key hurdles include the very definition and constitution of a democracy (barriers to entry and conditionality of exit); legal and regulatory differences; differences in domestic technological capabilities and attitudes toward corporate innovation, regulatory and financial provisions as well as strategic evaluation of technology and variations on strategic interests. It recommends that policy-makers in the West become increasingly aware of their own contributions to a global Splinternet, and instead continue a dual approach, whereby they address the tech-trade issues in one set of organizational arrangements, but pursue areas of interoperability in areas in which technological solutions will be vital to addressing questions of the global commons – climate, pandemic prevention, poverty reduction – with a continued, globalist attitude.

The battleground of technology

Technology has is now the pre-eminent battleground of economic leadership - and attendant to that political leadership – in an era of exacerbated great power competition. The conflict over Ukraine's sovereignty has placed a prism on the division between democratic and autocratic stewardship of the technology that will determine economic, political and human thriving over the coming decades, as the globe undergoes accelerated, sweeping transformations. In short: The IT stack is splitting along geopolitical fault lines. The nation – or nations – which best steer supply chains, acquire, adopt and mainstream emerging technologies such as AI, super- and quantum computing, 5G/6G and IoT based on digital networks, run over undersea cables or through independent cloud infrastructure, stabilized by satellite infrastructure while setting norms, rules and standards for technology to preserve privacy, security and system integrity from outside interference will create edge and hedging power for decades, where power overall has become diffuse.

How will governments negotiate or share power in geopolitical terms with their tech companies? Who assumes responsibility and political liability when things go wrong? Traditional instruments of market access limitations and regulation will prove too blunt a tool. To ensure a successful continuation of liberal democratic nations, countries who aspire to its values will have to cooperate in new ways, anchored in greater openness across sectors, to ensure that technological advantages are shaped toward democratic ends. More importantly, countries working together in this way, sharing sensitive knowledge and policy practice will need to be able to better assess and mitigate risk – both in traditional capital and investment terms – but also in terms of the very nature and definition of what constitutes and stabilizes democracies. In addition, democracies accelerating their collaboration must be aware of the dangers of "bloc building" themselves. Where technological innovation will be critical in addressing issues of the global commons – climate change, energy transformation, pandemic prevention, poverty alleviation – in the medium-term, democracies must be mindful of creating competitive systems that can create global norms and capacities.

This chapter will briefly retrace the development of the technological rivalry between Western countries and China, to examine the realities of early governance attempts across the continuous and rapidly evolving fields of technology, surveying efforts for their structural merits and evaluating them on their functional capacities and shortcomings. Gradual trust-building in regional and allied cooperation and the demands of urgency in competition with a burgeoning community of autocracies will likely create a web of minilaterals with a weighted node structure, rather than the formation of a more static or fully-fledged institutional design of inter-democratic technological stewardship – at least for now. These minilaterals – as illustrated in the chapter by Tyson Barker using the EU-U.S. TTC frame in this volume – will have to overcome a series of significant hurdles both in their substantive breadth, issue-bound overlap, internal power imbalances and in-group/out-group dynamics. Nonetheless, democratic partners should not lose sight of the possibility of building a group of vanguard tech democracies - a T-12 or T-14 structure - to work toward deepening advances on democratic principles in the protection and consolidation of telecommunications hardware, the protection of satellite, cloud and cable-based connectivity, and the interoperability of advanced software systems – all while signaling a desire to achieve "global commons" capacities in addressing threats with global consequences, where technology offers solutions.

The West and the Rest

The West's reaction to the "China challenge" has been two-fold – strategic outpacing and attempted hermetic closure – decoupling, friendshoring, or attempts at expediting "sovereignty" - fundamentally anathematic to the way in which corporate tech innovation has mapped its own global trajectory. Democracies and autocracies are in a moment of active competition for members of emerging technological coalitions on either side of a splintering internet and exacerbating competition over control of tech inputs, next generation networks and their stability, hardware sovereignty and software spread. This race to the bottom has taken its toll: overall internet freedom is in decline for the 12th consecutive year.[1]

Despite deep-seated systemic differences - and their articulation in norms, standards, technological products and usage - both democracies and autocracies will also need to find accommodation in areas of technological development between them for the feeder technologies that would have detrimental effects on human thriving – not unlike the development of nuclear technology and deployment. The possibility of weaponizing dependencies across the technological stack continues to have dangerous side-effects, particularly for those countries entirely tethered to third-country technology provision. Who – which institutions (following adaptation) and countries – will negotiate the "technological arms' deals of the future"?

The latter part of the chapter will thus examine possible trends in technology diplomacy around access and control as democratic governments expand their capacity to negotiate with one another on digital issues, interface with their own companies on the stewardship of fundamental technologies vital to public interest and national security and build multi-stakeholder arrangements nationally and internationally.

Open or Closed?: Technological leadership in a world of diffusing power

The promises of neoliberal globalization, which thrived based on cheap capital, cheap and quickly available energy, and outsourced - cheap – labor can no longer be fulfilled given the fundamental shifts in geopolitical relations between the two driving powers, China and the United States. Geoeconomic realities that have accompanied changing power relations alongside the realities of transnational challenges have introduced new break points on the structure of the global economy. These include shifting energy resources, changing mobility of goods and people (quickly evidenced for all to see during the pandemic), and the overarching need to accommodate the challenges of climate change. Taken together, they are posing urgent questions for the future of international order and the institutions that will mitigate, adjudicate, securitize and ultimately stabilize nation-state interactions in the future.

For decades, conventional wisdom dictated that open systems would win this century's innovation game: Open societies attracted the talent and economic inputs, marshalled and negotiated (in democratic processes) the government resources to produce advanced research and development and spurred the competitive environment and risk capital that brought innovative products to market: free markets, free speech, democracy – that combination would allow cross-sectoral advancement across a society in service of economic prosperity. Until the last decade, this recipe made the United States and its Western allies technological vanguards: The digital and communications revolution – as detailed by Jeremy Cliffe in this volume - swept the globe, with unbridled optimism – cementing American superiority.

The data revolution – with its emerging negative ramifications experienced first across the world through the capacities of US-built platform technology, quickly merging into the wider capacities of unregulated algorithms, created a disintegration of the concept of privacy and ever-expanding capacities of AI and revealed "new tech's" darker side. "Big Tech's" current $1 trillion valuation crisis seems a consequence of its overly optimistic global appetite – raising questions about technology as the savior of global growth.[2]

Most democracies have now fully awakened to the dangers that aspects of technology can pose to their values, norms and systems, even in their own hands – with democratic integrity and functionality challenged by outright cyberattacks on democratic infrastructure alongside the spread disinformation and its real-world consequences on democratic integrity across the globe. In a world in which information traveled at lightning speed, no nation-state – no matter how closed – would be able to retain an absolute monopoly on violence, security, information and financial flows. Western-built technology did not imply that its usage would be imbued with "western" values.

Systems designed to steer, decelerate, broaden and democratize decision-making – in short: democracy's bureaucracies - were simply overtaken by the speed of technological capacity and corporate greed to open and access markets, often with deep political and diplomatic implications:

Where in 2009 a State Department could still ask that corporate leaders of Twitter delay system-wide updates to allow Iranians to keep communicating with the world, by 2017 there was no more such government gatekeeping. Facebook's own market-opening efforts around "Free Basics" became a tool for genocide against the Rohingya in Myanmar. Parent company Meta is now subject to a $150 billion lawsuit for providing a "defective product" and acting with "negligence" – negligence that might be linked to 7,000 deaths.[3]

And where formerly owned government telecommunications providers couldn't keep up with sourcing the component infrastructure to build advanced networks, to power transformative 5G/6G technology at the speed of change, formerly-state owned operators now sought and signed – as Telekom/T-Mobile did in 2019 – near-ironclad contracts to continue purchasing Chinese-made hardware, against a shifting tide of geopolitical or national security concerns (and de facto now undercutting the current government's coalition agreement promises of "clean networks"), creating industrial dependencies not easily turned back.[45]

China's International Tech Footprint Expands

The last decade also proved a major fallacy in the assumption that openness, innovation and democracy lie at the heart of this recent technological revolution. China crafted its rival status in direct opposition to the Western model: by controlling its markets – inflow and outflow and its particularly-tiered corporate structure and by increasingly centralizing its authoritarian policies, developing strategies to expand its influence (from the BRI onward) and increasingly tightening restrictions on free speech. Despite recent economic shocks and slowing growth projections, China could still edge out the U.S. in achieving its 2025 AI and deep tech ambitions.[6]

Under the cover of its "Great Firewall" China retained the kind of global connections in R&D that would feed its circular economy and steered a progressive and sequenced acquisition of intellectual property and sufficient stake in Western (sub-)technology providers, component parts and machine-building capacities to control market inputs, develop rival technologies at scale to crowd out the few Western providers in the Chinese market over time and experiment with massive investments in risky technological innovation, including dual-use technology and quantum.[7] It has been nurturing its semi-conductor industry pro-actively, not least through its National Integrated Circuit Industry Investment Fund.[8] It accomplished all of this through central stewardship, while expanding the authoritarian control of its own population through mass surveillance technology (626 million facial recognition cameras covered the country by 2020), and while making the latter an export technology for its international footprint through the Digital Silk Road.[9]

"Open to the world but closed at home" - it effectively siphoned data from (BRI) client cities and countries across South America and Africa to build ever more sophisticated AI systems in line with its 2025 strategic ambitions,[10] while allowing leaders in the global South (and in Iran, Russia and parts of Europe) to actively suppress human rights, freedom of expression and democratic values, using tools "made in China." Today, the West's teenagers are addicted to China's TikTok, while their data (likely) moves seamlessly Eastward feeding closed AI development to improve surveillance[11], as well as the Chinese government's behavioral and political forecasting tools in full violation of data privacy policies painstakingly agreed by lawmakers. Only nine out of 27 European countries can boast "clean networks," marking continuous dependency, while the U.S. FCC has banned Chinese-origin electronics on national security grounds – but local telecom networks in the U.S. still aren't fully free of China-made components. An entirely uneven picture of stewardship, regulatory reach and international practice emerges.

The war in Ukraine has brought all these streams into direct confrontation: There, techno-democracies and their companies who – who have reframed corporate interests as their contribution to national, democratic interest - are actively engaged in the war effort. Much of Ukraine's resilience in the face of wiper, ransomware and DDoS attacks on the country's critical infrastructure, its networks, energy grids and hospitals, as well as the continued operations of its dispersed digital army and constant repairs to its Govtech apparatus, can be directly linked to contributions from Microsoft, Palantir and Starlink. The message? Democracy does not win without technology.

Squeezed by sanctions, abandoned by its IT elite and dependent on China for semi-conductors, military technology, and satellite back-up, Russia has actively embraced the deepening of a splinternet, which it began to pursue in active partnership with China in 2013 when the two countries signed news and information exchange agreement. The following years, leading up to February 7, 2022 "friendship agreement" between the Russian and the Chinese leaders served as a phase to consolidate their joint views of cyber "sovereignty" and attempt to push their vision of suppression of speech through technology (Putin signed on to a number of China's tech-driven playbooks for authoritarian rule), by advancing their unified vision of new global cyber order on the basis of Huawei IP protocol at the heart of the International Telecomms Union (ITU) and multilateral arenas from New York to Geneva.

Now, we see a hastening of the development of a sovereign yet joint Russo-Chinese internet model (part of China's "Great Rejuvenation"), supported by a wider Eurasian sphere including Iran, which has increased its purchase of Chinese surveillance technology to suppress current revolutionary energies.[12] The Sino-Russian information war has had measurable impact on the global interpretation of Russia's actions against its sovereign neighbor. And beyond the overheating semi-conductor race over the shortage of raw materials, Russia's war motivations are at least partially stoked by the $12.5 trillion valuated rare earth minerals deeply buried across embattled terrain in Eastern Ukraine.[13] Even to the future of the tech race, geopolitical and territorial control matters. The message? Autocracy does not win without technology.

Reconciling models of tech governance: Still fit for purpose?

These developments foreshadow what might still be to come. Over the past decade, Western governments have attempted to fortify their own systems along the entire tech stack, depending on their strategic needs, interests and capacities – from shifting hardware and industrial policies (clean networks), to curtailing the export of sensitive and dual-use technology, to stepping up oversight and regulation. While the struggle for democratic norms and standards has played out across multilateral fora – i.e. the UN Open-Ended Working Group on responsible behavior in cyberspace (OEWG) and in telecom standard-setting bodies, such as the ITU, which have seen direct face-offs between authoritarian and democratic leadership,[14] democratic countries have also been mapping out areas of collaboration and competition. With structural limitations in its competition with U.S. technology, the EU has developed a regulatory framework and led the U.S. in resolving critical and divisive issues on data privacy and storage. Between the development of the GDPR, the Digital Services Act (DSA) and the Digital Markets Act (DMA) designed to both widen and level the playing field for more competition to U.S. tech corporations, and a risk-first, human-centric approach to AI development and attempts to match the US in support for its semi-conductor industry and R&D environment to accomplish critical transitions ahead (green, energy, tech), the EU has discovered its added-value and institutional strength in democratic tech governance.

Europe's examples have led to a push to strengthen U.S. domestic institutions – the Federal Trade Commission, the Securities and Exchange Commission and the Committee on Foreign Investment – to eye stronger mandates – and despite a patchwork of privacy regulations across the U.S., an administration wanting to advance toward more comprehensive rules that would bring "the West" into greater alignment. The Biden administration has considerably deepened its political leadership on cyber, industrial tech competition and AI, in part through the creation of a "mission agency" in the National Security Commission on AI (NSCAI), discussed in greater detail below. India, too, now a pivotal tech actor, has pushed for internet governance rules and technical standards with international reach – by banning Chinese software and hardware and creating data localization laws. Further, Narendra Modi's government has created a New, Emerging and Strategic Technologies (NEST) division in its foreign affairs ministry, in part to oversee and coordinate their joint AI initiative (USIAI), their joint Science and Technology Forum (IUSSTF) and to feed joint conclusions stewarded through NEST into the Global Partnership on AI.

In addition to this unilateral deepening, an expanding number of bilateral formats – particularly around dual-use technology and defense issues – have proliferated between democracies, including in the U.S.-India Strategic Partnership (2+2 format), and more recently through ad hoc coordination on semi-conductor development between the U.S., Japan and the Netherlands. The development of a patchwork of cross-regional alliances – from the U.S.-EU Tech and Trade Council to the EU-India TTC, to Quad structures to a deepening of existing, specialized multilateral cooperation within NATO and among intelligence services.

Minilaterals – i.e. regionally focused, formalized multilateral constructs – have served the purpose of building trust over time, reducing heightened protectionist impulses, building confidence and "muscle memory" across disciplines and bureaucracies, in some cases laying the groundwork for sequenced and expanded agendas over time that may take minilaterals from coordinated industrial policy stewardship toward something more akin to strategic tech governance. But as Tyson Barker points out in his chapter on the EU-U.S. TTC in this volume, barriers of technological competition, issue-overload and issue-mixing continue to complicate negotiations.

But can an emergent patchwork of democratic alliances – even ones that could incubate and expanding agenda, like the EU-U.S. TTC as a weighted "node" around strategic technology collaboration be sufficiently quick and coordinated to compete with what closed systems (a Chinese-Russian-Iranian-Eurasian union) might be able to achieve and the deliberate and strategic way they might force others, dependent on their technology (not least its surveillance capacities), to embrace technology designed to curtail individual freedom and abrogate the principles of democracy that underpin international law?

From Minilaterals to a Tech-14? Scoping the breadth of democratic integration on strategic tech cooperation

Enter a broader thought: In 2008, U.S. policy planners in the Obama administration first floated the idea of creating greater strategic collaboration between the U.S and other leading countries committed to democratic values, leading to a series of cumulative Washington think tank initiatives. The Atlantic Council first pursued the collaboration of policy planners from 2014 onward – the year of Russia's illegal annexation of Crimea - now labeled as the D-10: Australia, Canada, France, Germany, Italy, Japan, South Korea, the United Kingdom, and the United States, plus the European Union charged with rethinking means to maintain democratic-led values-based international order – without tech as the center piece. Already, in-group/out-group dynamics proved complex, with India, Indonesia, Poland, and Spain participating as observers. Six years later the idea became central to the UK G7 Presidency with membership constituting the core members plus Australia, India and South Korea.[15] Later that year, it was coopted by U.S. President Trump as the primary venue to advocate for his “clean network” policy, to eliminate Chinese built 5G hardware from networks of associated democracies. As limited as this approach was in scope, it prompted a flurry of activity among UK and U.S. think tanks [16]and among advisors to the Biden campaign jockeying for position as he narrowed his international messaging around the threat of authoritarian countries to the international rule of law. A “Tech-10” (or later -12) could be the integrated yet flexible collaborative frame for democracies to counter the spread of ‘authoritarian’ hardware, disinformation, AI and leading-edge advances and the expansion of the tech race into space and back under water – satellites, cables and fundamental connectivity.

Whether or not China and Russia can form an expansive tech alliance on the back of the a Western sanctions regime forcing them together anew depends on a series of factors including a) the degree to which Chinese (and other) ICT companies and hardware providers expand into the vacuum left across the Russian tech market (from of Western technology companies, b) the ability of these other providers to skirt and the ‘techno-democratic’ global community’s ability to set and enforce an increasingly narrow tech-specific sanctions corset (from the Foreign Direct Product Rule (FDPR) and beyond), c) the capacity of Western governments and their technology corporations to link their affirmative tech hardware, infrastructure and connectivity plans meaningfully, particularly in Eastern Europe and key areas of the Global South – at speed – (B3W and Global Gateway) and implement these to push back against expansive efforts by Russo-Chinese collaboration and d) the ability of ‘techno-democracies’ – including the G7 states, Asian/Quad and South American partners – to mitigate unintended consequences of sanctions on digital connectivity in and to non-permissive environments, so that there is no unintentional acceleration or catalyzation of authoritarian consolidation of a sovereign internet. Speed is of the essence. There are sufficient “wedge” areas in which smartly aligned democracies could put a brake on a deepening authoritarian tech-empowered web.

These four points alone (and there are others) speak to a great – an urgent – need for “techno democracies,” to seek closer possibly even institutional coordination, knitting together the currently existent and partially overlapping approaches in existing, purpose-driven alliances (i.e. NATO; Five Eyes) and by deepening strategic cooperation in technology through bilateral, minilateral (i.e in multiple, sometimes coordinated, progressively deepening formats with various partners), full multilateral subject-based arrangements (OECD; OEWG/UN; ITU/UN) – or as suggested by some, through the creation of a separate alliance of technology-vested global democracies in a T-12.

A democratic tech alliance: T-12? Minilateral? Plurilateral? Multilateral?

Technologically advanced democracies are those with “skin in the game”: Democracies whose corporations, research institutions and private and government-funded innovation sectors produce key elements of today’s digital and tech infrastructure, and whose economic competitiveness increasingly relies on the flexible advancement of technology. These democracies are united in their commitment to rights-based, ethical deployment of technology, and regulation of technological assets withing a legal system capable of offering useful, clarifying legislation. The late April 2022 declaration on the “Future of the Internet” and its 60 signatories underscored how basic democratic premises might resonate with universal human rights: rooted in dignity, pluralism, open access, and economic empowerment for all people. But members of a Tech 10 or -12 would need to be able to go beyond declarations of intent and move – quickly – into action.

Democratic Stewardship of Technology: The difficulty of definitions

Defining the parameters and depth of (liberal, participatory, expanding) “democracy” in the ‘techno-democracy’ concept and the threshold for membership in an overarching, institutional arrangement has been – as of yet – the major stumbling block for widening of technological stewardship at scale. Digital governance practices in India, South Africa, and most recently Israel – possible qualifying members of a T-10/T12 coalition, can only be described as tending toward the illiberal. Within the EU, who would join member state governments (France, Germany, the Netherlands, etc.) in a possible alliance framework, leading member state politicians are actively courting Chinese surveillance and repression technology. Israel, with its undeniable technological advantages in intelligence gathering, dual-use development and start-up capacities did develop a new investment screening committee in 2020, but exempted investments in the tech sector from these evaluations, spurring the expansion of companies like Pegasus, which is hardly grounded in democratic principles. With the election of the most far-right government in the country’s history and its most recent attempt to weaken the country’s independent judiciary, its democratic “credentials” are waning.

To be a part of a T-12 alliance many leading tech democracies would need to work at home: Israel, Brazil, India and EU member states would have to negotiate their own relationships and dependencies on the Chinese market, sequencing and spacing decoupling efforts or seeking other means to keep sensitive data, intellectual property and tech manufacturing capacity out of China’s hands. The PHALCON and HARPY incidents around Israeli tech sales to China and its impact on Israeli-US relations read as a warning tale of just how difficult co-existence between tech superpowers can be, if capacity to agenda-set is limited.

Each of the possible “member” countries in such an alliance faces the challenges of vertical negotiations – leading tech countries, i.e. the US, UK, France, Israel and increasingly India – with their own corporations, whose power out of the hands of government control and supervision is having an impact on geopolitics. Further, it is entirely unclear which metrics would be used to evaluate the sustainability or “level” of democracy among possible member countries – though these metrics could be addressed. Finally, if trust-building and information sharing has been challenging in a minilateral setting, an expansion to a larger but flexible format could thwart instead of accelerate progress toward the joint goal of policy alignment.

From T-12 ambitions to minilateral realities: Creating inter-operable tech governance

If a T-10/12/x were to emerge as a global ambition, it would need to serve first as a clearing house for existing and developing initiatives across the G7/NATO/OECD/World Bank/UN, minilateral frameworks (all existing EU-US-India TTCs, QUAD and regional arrangements in Southeast Asia) and bilateral frameworks (U.S.-Japan, U.S.-India) and usefully clarify in-group/out-group dynamics in its relations with non-democratic tech leaders, including Singapore and Indonesia.

A multilateral clearing-house structure of this nature would need to be capable both of scaling majoritarian initiatives (potentially emerging from minilaterals), while avoiding duplication, increasing functional interventions (against disinformation; supporting democracy protection) and create a series of negotiation and exchange platforms on data protection, privacy and privacy-enhancing technology and risk capital securitization to

- create deeper technological convergence (R&D sharing; semiconductor design, etc.) considering tech advances in authoritarian systems
- establish functional risk mapping and early warning systems to protect vital joint interests (hardware systems and international critical digital infrastructure, including undersea

cables); securing 5G and 6G tech can be sourced from democratic countries, at scale and at competitive price points

- develop and promulgate international norms and standards on ICT hardware, software and AI under democratic guidelines to be applied through existing bodies
- map supply chain vulnerabilities and shortfalls in critical inputs (including for lithium, nickel and rare earth minerals); create a democratically monitored reserve structure
- develop a certification program for high-quality infrastructure and tech projects [as part of global development agenda]
- coordinate mechanisms for dual-use export control and verification of tech imports (particularly in the burgeoning smart cities and surveillance tech market)
- provide sanctions guidelines for T-12 corporations mitigate unintended consequences that could hasten authoritarian consolidation of a sovereign (Sino-Russian) internet
- exchange intelligence on scaled disinformation and disruption of major data flows i) expand the existing "grand challenges" projects on 'democracy affirming tech' to a global scale.

Secondary ambitions might include the protection of T-12 cities from the overreach of authoritarian/surveillance technology providers into the Smart City space (a market now valued at over $800 billion annually), which could be 'backdoors' to creating significant damage in democracies, both in critical infrastructure and democratic discourse. The coordination of global funding resources could be a further secondary ambition: The 2018 MOU between Australia, Japan and the US to collectively source private capital to fund major regional infrastructure projects (effectively a precursor to the B3W plans of the Biden administration), including the 2020 internet cable to Palau is a model of potential projects to emerge from closer coordination between democratic countries on structural network provision – beyond minilateral structures. In Cape Verde, where cables from North America meet European and African cables, the race for control is clearly on.

For all of the need, the hurdles are similarly real: Divergent threat perception and market dependencies have led to a preference for bilateral or minilateral cooperation around a circumscribed set of priorities that also level playing field of leadership toward greater parity and functional, practical exchange. Legal precedence, questions around leadership structure, fear of duplication, existing trade agreements with in-built market protections, intelligence and political statutes and structures, and stark differences in technology culture and degree of technological capacity, and competitor status among possible T-12 "members" alongside fears of "further antagonizing China," are some of the main reasons political dynamism has not aggregated around elevating nascent collaboration on a wide spectrum of technology issues to this level. Failure of the idea to pick up momentum speaks not solely to the breadth and depth of barriers, but rather to the fact that trust-based organization forms must both be scoped correctly and have a measurable function to create social and organizational capital over time. For example, a potential T-12 precedent, the D5 – UK, S. Korea, Israel and New Zealand – focused on GovTech, CiviTech and OpenTech best practice exchange, has taken six years to develop into D9, building on common values, pooled knowledge and gradual trust building.

As useful as it is to chart the possibilities of a structured T-10/12, "weighted nodes" of collaboration in minilaterals, where members which overlap must take care to avoid policy duplication and alignment is likely "as good as it gets" for the medium term. As Tyson Barker describes in this volume, the EU-U.S. Tech and Trade Council could be such a node.

it has quickly redeemed itself to become a multi-agency, multi-sectoral negotiation framework and clearing house, focused on mapping, regulatory impact management, resource pooling, information sharing and the often-delicate negotiation of subsidies and (tech)-expansionary use of trade tools for common objectives. Within a year of its existence, it had additionally become a forum for multi-stakeholder negotiations of tech-adjacent policies with ramifications for international competitiveness, adding formats to address issues of mutual agreement and contention, such as the impact of the US CHIPS Act and the US Inflation Reduction Act on the freedom of operation for European companies, pointing to the fact that it could also be seeding the bases of a new transatlantic trade pact.

Its capacity to act as a trust-building venue after the erosion of transatlantic collaboration in the Trump era made it exemplar in its design: The EU-India TTC will not only follow similar structural make-up but be sequenced to interact with the EU-U.S. TTC, to avoid duplication of efforts and a stripping of resources. Similarly, there are early indications that the Indian 2+2 format with the United States, encompassing foreign, intelligence, military and science collaboration in a bilateral format, will be framed to connect more seamlessly to EU-U.S. and EU-India TTC provisions. In addition, nothing bars TTC working groups from at least informally exchanging with the two QUAD structures on critical emerging technology and defense technology, and numerous bilateral structures focusing on specific digital policy subsets.

Core elements of the EU-U.S. TTC could similarly serve as a model to expand coordinated tech governance to Latin America and the Caribbean, under European leadership, as Jose Ignacio Torreblanca and Carla Hobbs have argued as a priority under the Spanish Presidency of the EU in 2023. [17] Distilling from the lessons around trust-building, values ascertainment, transferability of regulatory framework tools (particularly around data security and privacy), and practical knowledge-sharing (i.e. rare earth mapping, sustainable mining) from the existing “node” structure in in the EU-U.S. TTC will facilitate the successful establishment and maintenance of this minilateral.

Rethinking Diplomatic Intelligence for Techno-Democratic Stewardship

Gaining and defending ground for techno-democracies, no matter in what forum – closed multilateral, global multilateral, sequenced minilateral – will demand an expansion of diplomatic practice, one that mimics the corporate development cycle for tech applications or products – from mapping and foresight, to risk analysis and gaming, open and closed lab structures (or in the language of diplomacy: functional Track 1.5 and 2 dialogues) with greater tolerance for risk and error, but focused on means to achieve both better technology outcomes from the exercise of diplomacy and to build regulatory capacity from the ground up, to continue to expand the translation of democratic norms and values in legislation across all forms of governance, from nation-state to multilateral fora.

Building diplomatic and regulatory capacity begins with priority setting and executive signaling. The Biden administration telegraphed its seriousness on integrated tech policy across departments by elevating the Office of Science and Technology Policy to cabinet level.

Most recently, Japan, the U.S. and the UK used their individual national security-, defense- and technology/cyber strategies to send a similar signal: Technology – hardware, software, defense and societal applications, digital rights – flow like a plumb line through these documents.

Negotiation tables of the future will have to be structured vastly differently, if the wider intention might be to use “minilateral” formats to advance toward a “T-x structure” of techno-democracies. It will require a cross-systems approach that builds in vertical negotiation with a country’s own corporations and their activities abroad.

It will also require figuring out how diplomatic knowledge about all aspects of technological development, usage, dependencies, etc. about the “other” is shared within network. Where China’s CICIR can simply and centrally plan, synthesize and analyze multi-sector conversations (even those in a Track 1.5/2 format) for strategic purposes across all domains of data diplomacy – in part using AI for data analytics – in their “sovereign” domain and with partners, techno-democracies will have to lean toward increased openness – and more inclusive formats for their advantage. [18] As Madeline Carr argues “China has a comprehensive insight into all other states that engage with it, whereas we have only our own.” China uses over 30 methods, both licit and illicit, and a diverse cadre of actors to gain access to non-native technology.

Devising common regimes that can then allow for regulation that is both sufficiently narrow, as to not impede corporations and the industrial base and achieve long-term national security goals is difficult enough at home, as evidenced by ongoing negotiations around a functional outbound investment screening mechanism for critical technology in the U.S.[19] Elevating these discussions to the multi-lateral level with the EU or Japan (or the EU with India) seems near impossible if earliest stages – including the diplomatic assembly of working groups – are not conceptualized in an interagency format, with outside expertise and constant corporate cooperation. The Quad Cybersecurity Joint Principles and the working group structures of the EU-U.S. TTC establish norms of this structured cooperation and are examples in this regard.[20]

The greatest value of the minilateral structure moving toward weighted notes of a T-x collaboration, as discussed above, could well be in achieving a more complete picture of the array of challenges, vulnerabilities and possibilities facing techno-democracies. This has already begun as part of the EU-U.S. TTC framework and through domestic R&D investments of a different sort, with a mapping of rare earth materials as agreed as the May 2022 Saclay meeting, with a decision on strategic overland and subsea cable connections (beyond potentially Cape Verde) as confirmed in December 2022 and in the diagnostic work for the alignment and resiliency of Global Gateway and B3W projects. Individual partners have already developed scalable diagnostic structures, including the EU’s 5G Toolbox and the U.S National Network for Critical Technology Assessment or the new Directorate for Technology, Innovation and Partnerships at the country’s National Science Foundation conceptualized particularly to probe for weaknesses in the country’s supply chains and delineating emerging challenges to be solved by the better application of edge technologies.

Recommendations for the near-term future

If leading techno democracies pursue an ideologically-centered governance architecture, they must realize such an initiative could similarly signal authoritarian governments to accelerate their own splintering efforts, when challenges of the global commons – climate change, pandemic prevention, supply-chain integrity – will demand interoperable technological solutions for global progress.

In fact, on certain issues – both domestically and internationally – democratic governments should be embracing radical openness, instead of closure, to advance.

Forming “mission agencies” at home, like the multi-sector National Commission on AI (NSCAI), imbued with the authority of the Executive, but with a multi-stakeholder approach and a singular objective, organizations like this can catalyze policy implementation, including passing legislation and creating structures to catapult U.S. AI capacities into the future. The NSCAI and the concept of mission agencies in general should serve as the blueprint for Germany's "Alliance for Transformation," and other such consortia emerging across the European Union, for example, dedicated to thinking technological challenges down to the core, including to changes in the education systems across democracies.[21]

Secondly, techno-democracies should – in part because the challenges are so rife and arriving at such speed – should avoid creating duplicative structures at all costs. Instead, particularly when it comes to the urgent need to reform national foreign policy and intelligence structures as outlined above, they should be comparing notes. Australian National University's Tech Policy Design Center and its database of tech policies from 40 countries can help other democracies looking to make efficient policy-design choices that can support both the deepening of minilateral structures and can support the creation of a "floor" toward the construction of a wide tech governance structure.

Finally, the strength of global democracies – regardless of the stage of their democratic development – lies in their openness, and ability to establish values and norms even in working consortia such as these nascent tech governance structures. The ability to use collaborative formats to build "in network" stickiness, delivering 'proof of concept' to restore a modern version of the liberal democratic promise to guarantee physical and economic security alongside expanded democratic rights of free expression and participation in the digital sphere will create its own power. To use that power systematically (against the threats wielded by autocracies against these principles with the tools of the digital age), democracies will need to adapt and redefine their notions of collective governance and control.

These are massive changes in bureaucratic and political practice, particularly in a world in which democratic openness has spurred overheating capitalist gains from technological advancement. Quickly, democracies will have to learn how to negotiate power with their own corporations, or risk mimicking regulatory approaches that force companies into line (the Chinese way) but reduce the innovative capacities that define democracies. The choices are as real as they are stark – and above all, urgent.

Endnotes:

1 Freedom House. (2022). Freedom on the Net: Countering an Authoritarian Overhaul of the Internet. December 2022.

2 Mickle, T., Weise, K., & Grant, N. (2023). Tech's biggest companies discover austerity, to the relief of investors. New York Times. February 2, 2023.

3 Culliford, E. (2021). Rohingya refugees sue Facebook for $150 over Myanmar violence. REUTERS. December 8, 2021.

4 Pleming, S. (2009). U.S. State Department speaks to Twitter over Iran. REUTERS. June 16, 2009.

5 Cerulus, L. (2022). Germany is (still) a Huawei hotspot in Europe. POLITICO. December 14, 2022.

6 Dawson, J., & Wheeler, T. (2022). How to tackle the data collection behind China’s AI ambitions. Brookings Institution. April 29, 2022.

7 Sheehan, M. (2023). How China became an Innovation Powerhouse. Carnegie Endowment. January 10, 2023.

8 Larsen, B. C. (2022). The Geopolitics of AI and the rise of digital sovereignty. Brookings Institution. December 8, 2022.

9 Keegan, M. (2019). Big Brother is watching: Chinese city with 2.6m cameras is world’s most heavily surveilled. The Guardian. December 2, 2019.

10 MERICS. (2016). Made in China 2025: The making of a high-tech superpower and consequences for industrial countries. December 2016.

11 Chee, F. Y. (2023). TikTok CEO seeks to reassure EU on privacy, child safety. January 10, 2023.

12 Khorrami, N. (2022). How China boosts Iran’s Digital Crackdown. The Diplomat. October 27, 2022.

13 Faiola, A., & Bennett, D. (2022). In the Ukraine war, a battle for the nation’s mineral and energy wealth. Washington Post. August 10, 2022.

14 Wheeler, T. (2022). The most important election you’ve never heard of. Brookings Institution. August 12, 2022.

15 Ichihara, M., & Brattberg, E., & Judah, B. (2020). The D10 Initiative and Japan: Options for Expanding the Coalition of Democracies. Nippon.com. August 16, 2021.

[16] Manuel, A. (2020). The Tech Ten: A flexible approach to international tech governance. Blogpost.

[17] Hobbs, C., & Torreblanca. (2022). Byting Back: The EU’s digital alliance with Latin America and the Caribbean. ECFR Policy Brief. October 24, 2022.

[18] Carr, M. (2022). Tech Policy Dialogue in Times of Geopolitical Tension. Unpublished conference paper (delivered at the CNAS T-12 Track II convening in Paris, France). May 2022.

[19] Benson, E., et.al. (2023). Transatlantic Approaches to Outbound Investment Screening. CSIS. January 17, 2023.

[20] Ministry of Foreign Affairs, Japan. (2021). Quad Cybersecurity Joint Principles.

[21] NSCAI Mission. (2021). On the principle of “Mission Agencies,” see Bertelsmann Stiftung. (2023). Deutschland transformieren: Missionsagenturen als innovativer Baustein zur Bewältigung gesellschaftspolitischer Herausforderungen. February 2023.

4. The EU: A force for (digital) good? José Ignacio Torreblanca

Freedom House has documented 16 straight years of democratic decline around the world.[1] The result is that consolidated democracies are devolving into the illiberal. "Born again authoritarians" countries like Turkey that once had democracies and have regressed are no longer the exception. And, as the cases of Hungary and Poland prove, the decline is happening even at the very heart of the European Union, which claims to be the most advanced space for democracy in the world.

This global democratic decay represents a major geopolitical challenge for the EU, which has an existential interest in sustaining the multilateral liberal international order. As the President of the European Commission, Ursual von der Leyen, has pointed out, multilateralism, synonymous with a law-based order, is in the EU's DNA: it underpins its security and prosperity. However, as the EU has experienced only too well over the past decade, without liberal states (at home) a global liberal order is not possible: illiberal states and authoritarian regimes conceive of the international order as a destabilizing element from which to isolate themselves or in which to participate exclusively according to a logic of power.

In addition to the decline in the number of democracies, there are two interrelated phenomena that profoundly weaken democracy: increased political polarization and the loss of faith in elections. As we have seen in the U.S. with the assault on Capitol Hill and in Brazil when the three branches of government were stormed, the combination of both elements makes for a very dangerous cocktail.[2] This involution is the consequence of the systematic destruction of communicative, media, and political representation spaces of our societies as a result of the disintermediation facilitated by the new information and communication technologies, i.e., social platforms and networks.

The decline of democracy goes hand in hand with the rise of digital authoritarianism. On the one hand, authoritarian regimes are increasingly effective in suppressing dissent and controlling social networks.[3] These regimes have found in the horizontal and open nature of these networks and in their inadequate or non-existent regulation in many countries, a vulnerability to exploit against democracies. Data shows that between 2014 and 2020, 1.7 billion people in 33 countries voted in elections that were interfered in by foreign powers.[4] They also experienced large-scale COVID-19 disinformation aimed at destroying public confidence in authorities, experts, institutions, and the media.[5]

The war in Ukraine provides a telling example of how vulnerabilities in the information space can become geopolitical and security weaknesses. In the months leading up to the invasion, the Russian disinformation machine was able to counter US warnings about the intentions of the Russian military deployment quite effectively. Strategies of denial, ridicule, and delegitimization helped to shape public opinion and encouraged European governments into believing that the military intervention was a US propaganda operation to stigmatize Russia, when its real goal was to prevent both NATO and EU partners from fully committing to the defense of Ukrainian sovereignty.

It is true that Ukraine has subsequently been able to build a very powerful narrative of its will to resist, which in turn has allowed it to sustain its war effort and garner vital moral and material support for resistance to the Russian invasion. At the same time, however, European authorities have found that outside EU borders, in what many refer to as the "Global South", Russia has been very successful at undermining the legitimacy of the European and US response. Although the Russian military has suffered severe defeats on the ground, as EU High Representative for Foreign and Security Policy Josep Borrell has noted, when it comes to the battle of narratives, the EU has been losing.[6]

The European response to this challenge is insufficient in large part because this challenge is being waged in the field of information and communication on social networks, whence the European Union and member states are neither fluent nor competent. In his recent speech to EU ambassadors meeting in Brussels in December 2021, Mr. Borrell rightly lamented the reactivity, lack of presence, and ineffectiveness of European diplomacy in the global conversation about Ukraine and encouraged them to join the battle of narratives.[7] As one diplomat in the room rightly replied: "we are being asked to respond to an industrial disinformation operation by tweeting a little more every day." The EU's frustration is understandable, but to overcome Brussels will need to understand how and why it is in this situation.

The EU has taken some important steps in regulating social media already. In 2018, it published its first communication on disinformation.[8] It then invited large platforms to join a process of information sharing, transparency, and best practices through which it was able to get companies to start actively engaging in and be held accountable for taking down fake accounts, detecting coordinated inauthentic behavior, and monitoring the truthfulness and authenticity of political advertising. With the approval of both the Digital Services and Digital Market Acts (DSA and DMA), the EU has shown great determination and vision to contain the most damaging effects of social media platforms and networks on democracy. In this task, it has undoubtedly been helped by the pandemic, which has made clear that disinformation can have a powerful impact on public health and should be considered a social risk of the first magnitude. As a result, society, the media, public opinion, and governments have changed their perception of the risks associated with social networks and begun to act within their respective spheres of competence to counteract these trends.

Two criticisms of the EU that should be flagged are that this determination has been inward-looking and primarily defensive, rather than offensive or proactive. The result is that globally, starting with the U.S., the lack of or inadequate regulation of social networks continues to threaten the integrity of democracies and their communicative and deliberative spaces.

The EU cannot be triumphalist. Its program of strategic autonomy or (more ambitiously) "digital sovereignty" is far from complete when it comes to preserving democracy from the misuses and abuses of technology. On the one hand, the regulatory success of such rules as the DSA remains to be demonstrated in practice: its deployment and implementation will be slow and fraught with difficulties, both on the part of governments (since member states bear a large part of the responsibility), and of social platforms and networks, whose commitment to this regulatory agenda, as the cases of Tik Tok and Elon Musk's takeover of Twitter show, are weak, fragile or non-existent.

On the other hand, European initiatives to fight this global battle of narratives need a major update. The pioneering anti-disinformation service launched by the EU's External Action Service, East StratComm, built a catalogue of nearly 15,000 pieces of Russian-sourced disinformation [euvsdisinfo.eu]. This repository has educated a whole generation of politicians, journalists, and experts on the complexities of disinformation narratives, but this massive effort is proving to have the same limitations as the fact-checking processes undertaken by civil society and the media. Disproving or classifying information as false is necessary, but this disproval does not automatically reach the people who consumed the disinformation; they are located in communicative bubble-spaces that are immune to these processes. Verification neither acts on the ecosystem in which disinformation is disseminated nor acts at source against those responsible for its creation and dissemination. It is, therefore, a partial and very incomplete tool.

Acting on the digital ecosystem requires well-honed legal capacities, and herein lies the importance of the DSA. Acting at source is especially complicated because whereas the EU adopts a defensive, legalistic, and protective position to establish attribution processes based on empirical evidence and the use of legal instruments (police, prosecutors, judges and courts), the actors that develop influence strategies act offensively and with long-term strategy according to a logic of power and conflict that in many cases is analogous to that of warfare. As RT's director Margarita Simonyan revealed, Russia's networks of influence and interference are not spontaneous: over the last few years, Moscow has developed a long-term strategy to create and cultivate loyalty among audiences in the West who could be mobilized at critical moments to defend its positions, weaken the Western consensus, and delegitimize its messages and institutions.[8] Such a long-term media strategy that includes TV channels as well as digital and social media is something the EU lacks (and is hardly available to a government apparatus in a democratic society). Thus, in its fight against the abuse of technology to undermine democracies, the EU is doubly hamstrung by a defensive and legalistic logic that prevents it from acting proactively and in accordance with a geopolitical and security logic. What can it do about this and what is it doing?

As a result of reflection on the EU's insufficient external activism in digital matters and concerns about both the growing intersection between geopolitics and technology and the rise of digital authoritarianism, the EU adopted its first external digital diplomacy in July 2022.[9] This strategy sets out the need for the technological and digital component as a central element of the EU's external action and aims to combine and coordinate under a single strategy element of political action that have hitherto been scattered, e.g., external action aspects of the cybersecurity strategy, the action plan on democracy or the fight against hybrid threats, including foreign information manipulation and interference (FIMI).

In addition to this coordination, the Council invited the Commission and the High Representative to work closely with like-minded countries, both bilaterally and regionally, and multilateral organizations to maintain an open, free, global, stable, and secure Internet based on a multi-stakeholder approach. In doing so, the EU consolidates its vocation to the global governance of technology with the aim of imprinting on this governance its humanist and rights-based vision of technology or, as the Council puts it, the shaping of "ethical, safe and inclusive international technology standards." Special attention should be paid to the expression of the will to act on "countries of strategic importance that have a high level of vulnerability," to combat Internet shutdowns, arbitrary or indiscriminate digital surveillance and data retention, to protect human rights defenders and civil society online, and to expand civic spaces.

This is an ambitious agenda that requires coordination between multiple levels both within the Commission and between European institutions and organizations. Just as important, if not more so, is that such a strategy requires close and in-depth dialogue with third actors, both bilaterally and multilaterally. Some, e.g., the Trade and Technology Council (TTC) with the United States and digital partnerships with Japan, Canada, and Korea, are already underway. The EU has also shown its vocation to coordinate its strategies with Indo-Pacific countries, the African Union, and Latin America and renew its cooperation in the framework of such organizations as UNESCO, the ITU and the OECD.

If the EU is to become this "force for digital good," it will have to go much further. As has been said many times, the weight, power, and attractiveness of its internal market turns the EU into a de facto regulatory superpower. The accumulation of legislation on digital and technological matters approved by the EU in recent years that covers everything from data to AI, digital markets and services, and cybersecurity undoubtedly makes the EU the most densely regulated digital and technological space in the world and a benchmark for many countries (not least of which the U.S.) to imitate.

Ideally, with all these regulations in place and with their successful implementation, the EU would be in a position to claim to have achieved its desired goal of strategic autonomy (or, at least in part,”'digital sovereignty”). With respect to the rest of the world, it could rely on the “Brussels effect” popularized by the conversion of its European data regulation (GDPR) into the global data gold standard. But would that be enough? Or credible? As with security, the risks and threats posed by technology are not divisible in a global market and such a conflict-ridden geopolitical environment. As in so many other matters, even if it could, the EU cannot aspire to standards so high that by their very cost and nature they are unattainable by the rest of the world. A “Galapagos effect” that renders the EU so advanced in its rules that it cannot relate or deal with anyone is simply not possible nor desirable.[10] The EU must therefore think in terms of global governance. This requires seeking to empower third parties, be they governments, parliaments, independent institutions, civil society, or experts outside Europe.

One of the great difficulties in this task is the relationship with the U.S. In a world dominated by geopolitical rivalries and high-voltage tensions between the West on the one hand, and China and Russia on the other, there is not enough room for two models of digital governance as opposed to each other as the European and the US. In an ideal world, the U.S. and the EU should be able to design together with other like-minded OECD and Global South countries a digital governance architecture equivalent to the Bretton Woods system achieved after World War II. If back then an international liberal order was tailored to merge and satisfy both the material needs and the moral aspirations of liberal democracies, the challenge today would be to achieve a multilateral digital liberal order compatible with liberal values, or at least as broad a sphere of rights-based technological governance as possible given that China and Russia would refuse to be part of such an order.

The US polarisation precludes Washington from becoming a driving pillar of such rules-based global governance. And even if legislation matching the EU was approved by the Democrats or through bipartisan agreements, uncertainty about the reversibility of any international agreements the U.S. might eventually commit itself to would be very high. Although many domestic actors in the U.S. (states, cities, civil society) aspire to this regulatory convergence with the EU that could eventually become a template that could be extended globally, the difficulty of bi-partisan consensus and the classic reluctance of the executive and legislative branches to reach internationally binding agreements make it very difficult to take this first step. For this reason, although agreement between the

U.S. and the EU is not a sufficient condition for global governance, it is a necessary one.

There is a plethora of actors in the Global South and the G-20 orbit (India, Brazil, and others) whose cooperation and contribution are also essential. For both the U.S. and the EU, talking and agreeing with these actors is extremely difficult not because their alignment with democratic and liberal values is weak or fragile (where are they not nowadays?: let he who is blameless cast the first stone) but because their vision of international order and global governance is mediated by their past negative experiences with the West. Many of these countries conceive of the multilateral order as a purely Western artifact aimed at safeguarding Western power and excluding others. Their participation in such an enterprise cannot be taken for granted.

Convergence among democracies must come from below and not from above. Actions speak louder than words such that when countries see the tangible benefits of such a model, they will make it their own out of pure self-interest. Just as after the Second World War, when the U.S. and the other liberal democracies managed to fit their economic and security interests into a multilateral framework that was also liberal, the challenge for the EU today is to offer liberal democracies a model of embedded multilateralism in terms of global internet governance. As a matter of both interest and principle, the EU's DNA demands the same approach to the governance of technology as to health or the environment: as a global public good to the provision of which it contributes decisively, even if unilaterally at first to establish a tit-for-tat model of cooperation. Just as God can write straight with crooked lines, the EU can unilaterally promote technological governance in the interest of all by going solo at the beginning (or so should we hope and invite it to do).

Endnotes

[1] Freedom House. (2022). Freedom in the World 2022: Global Expansion of Authoritarian Rule, https://freedomhouse.org/report/freedom-world/2022/global-expansion-authoritarian-rule

[2] European Council on Foreign Relations. (n.d.). Power Atlas: Culture, https://ecfr.eu/special/power-atlas/culture/#weaponising-the-vulnerabilities-of-other-systems-rather-than-being-a-city-on-a-hill

[3] Freedom House. (2022). Freedom on the Net 2022: Countering the Authoritarian Overhaul of the Internet, https://freedomhouse.org/report/freedom-net/2022/countering-authoritarian-overhaul-internet

[4] Australian Strategic Policy Institute. (n.d.). Cyber-enabled foreign interference in elections and referendums, https://www.aspi.org.au/report/cyber-enabled-foreign-interference-elections-and-referendums

[5] Facebook. (2021). IO Threat Report May 20, 2021, https://about.fb.com/wp-content/uploads/2021/05/IO-Threat-Report-May-20-2021.pdf

[6] European External Action Service. (n.d.). G20: Difficult times for multilateralism, https://www.eeas.europa.eu/eeas/g20-difficult-times-multilateralism_en

[7] European External Action Service. (2022). EU Ambassadors Annual Conference 2022: Opening speech by High Representative Josep Borrell, https://www.eeas.europa.eu/eeas/eu-ambassadors-annual-conference-2022-opening-speech-high-representative-josep-borrell_en

[8] EUvsDisinfo. (2018). Chief Editor: RT is Like "a Defence Ministry", https://euvsdisinfo.eu/chief-editor-rt-is-like-a-defence-ministry/

[9] Council of the European Union. (2022). ST 11406 2022 INIT, https://data.consilium.europa.eu/doc/document/ST-11406-2022-INIT/en/pdf

[10] *idem.*

5. Rethinking Democratic Tech Governance in the Euro-Atlantic: A TTC Progress Report. Tyson Barker

Abstract

This paper examines how the digitisation of information and the emergence of social networks have resulted in the weakening of liberal democracies and, in parallel, the strengthening of authoritarian regimes. To counteract the ability of foreign actors to disseminate narratives that delegitimise democracy, it proposes that the European Union should lead a grand multilateral agreement that, in the manner of Bretton Woods, establishes the framework for a democratic governance of technology.

The weaponising of information against democracies

Freedom House has documented 17 straight years of democratic decline around the world[1]. The result is consolidated democracies devolving into illiberal. The "born again authoritarians" countries like Turkey, which, having enjoyed democracies, have regressed, are no longer the exception. And, as the cases of Hungary and Poland prove, the decline is something happening even at the very heart of the European Union, which claims to be the most advanced space for democracy in the world.

This global democratic decay represents a major geopolitical challenge for the EU, which has an existential interest in sustaining the multilateral liberal international order. As the President of the European Commission, Ursula von der Leyen has pointed out, multilateralism, synonymous with a law-based order, is in the EU's DNA: it underpins its security and prosperity. However, as the EU has experienced only too well over the past decade, without liberal states (at home) a global liberal order is not possible: illiberal states and authoritarian regimes conceive the international order as a destabilising element from which to isolate themselves, in which to participate exclusively according to a logic of power, or, even, an existential threat they thus have to undermine.

Among the various elements negatively impacting on the quantity and quality of democracies, it is worth highlighting two interrelated phenomena that profoundly weaken democracy: one, the increase in political polarisation and, second, the loss of faith in elections [2]. As we have seen in the US when the assault on Capitol Hill and in Brazil when the three branches of government were stormed, the combination of both elements makes for a very dangerous cocktail. This involution is the consequence of the systematic destruction of communicative, media and political representation spaces that our societies have been experiencing as a result of the disintermediation facilitated by the new information and communication technologies, i.e., social platforms and networks.

The decline of democracy goes hand in hand with the rise of digital authoritarianism. On the one hand, authoritarian regimes are increasingly effective in suppressing dissent, controlling social networks and exporting surveillance technologies to third countries [3]. These regimes have found in the horizontal and open nature of these networks, as well as their inadequate or non-existent regulation in many countries, a vulnerability to exploit against democracies. Data shows that between 2014 and 2020, 1.7 billion people in 33 countries voted in elections which were interfered by foreign powers[4].

Democracies have also experienced large-scale COVID-19 disinformation processes aimed at destroying public confidence in authorities, experts, institutions and the media[5].

The war in Ukraine has provided a good example of how vulnerabilities in the information space do not only harm democracy at home but can turn into major geopolitical and security weaknesses. As we saw, in the months leading up to the February 24th, 2022, agression, the Russian disinformation machine was able to globally counter US warnings about the intentions of the Russian military deployment quite effectively. Strategies of denial, ridicule and delegitimisation helped to shape public opinion and European governments into believing that the military intervention was a US propaganda operation aimed at stigmatising Russia, when its real goal was to prevent both NATO and EU partners from fully committing to the defence of Ukrainian sovereignty.

It is true that Ukraine has subsequently been able to build a very powerful narrative of its will to resist, which in turn has allowed it to sustain its war effort and garner vital moral and material support for resisting the Russian invasion. At the same time, however, European authorities have found that outside EU borders, in the so-called 'Global South', Russia has been very successful in undermining the legitimacy of the European and US response. While on the ground the Russian military has suffered severe defeats, as EU High Representative for Foreign and Security Policy Josep Borrell has noted, when it comes to the so-called 'battle of narratives', the EU has been on the losing side[6].

The EU counter disinformation efforts

The European response to this challenge is insufficient in large part because is being waged in a field, that of information and communication on social networks, in which the European Union and member states are not fluent or competent. In his recent speech to EU ambassadors meeting in Brussels in December 2021, Mr Borrell rightly lamented the reactivity, lack of presence and ineffectiveness of European diplomacy in the global conversation on Ukraine and encouraged them to join the battle of narratives[7]. However, as one diplomat in the room rightly criticized: ‘we are being asked to respond to an industrial disinformation operation by tweeting a little more every day’. The EU’s frustration is understandable, but to overcome it Brussels will need to understand how and why it has reached the situation it finds itself in.

So far, the EU has taken important steps in regulating social media. In 2018 it published its first communication on disinformation[8]. It then invited large platforms to join a process of information sharing, transparency, and best practices through which it was able to get companies to start actively engaging and being accountable in taking down fake accounts, detecting coordinated inauthentic behaviour (CIB), monitoring the truthfulness and authenticity of political advertising. Finally, with the approval of both the Digital Services and Digital Market Acts (DSA and DMA), it has shown great determination and vision on the need to contain the most damaging effects of social media platforms and networks on democracy. In this task, it has undoubtedly been helped by the pandemic, which has made it clear that disinformation can have a powerful impact on public health and therefore should be considered a social risk of the first magnitude. As a result, society, the media, public opinion, and governments have changed their perception of the risks associated with social networks and have begun to act, within their respective spheres of competence, to counteract these trends.

However, if there is one criticism that could be flagged on the EU it is that this determination has been inward-looking, and that it has been primarily defensive, not offensive, or proactive. The result is that globally, starting with the US, the lack of or inadequate regulation of social networks continues to make them a threat to the integrity of democracies, their communicative and deliberative spaces.

The EU cannot be triumphalist. Its programme of strategic autonomy or (more ambitiously) 'digital sovereignty' is far from complete when it comes to preserving democracy from the misuses and abuses of technology. On the one hand, the regulatory success of rules such as the DSA has yet to be demonstrated in practice: its deployment and implementation will be slow and fraught with difficulties, both on the part of governments (since member states bear a large part of the responsibility), and of social platforms and networks, whose commitment to this regulatory agenda, as the cases of Twitter after the takeover by Elon Musk and Tik Tok show, are weak, fragile or non-existent.

On the other hand, European initiatives to fight this global battle of narratives need a major update. The pioneering anti-disinformation service launched by the EU's External Action Service, East StratComm, has built a catalogue/repository of nearly 15,000 pieces of Russian-sourced disinformation. This has educated a whole generation of politicians, journalists, and experts on the complexities of disinformation narratives. However, this massive effort is proving to have the same limitations as the fact-checking processes undertaken by civil society and the media. Disproving or classifying information as false is necessary, but this disproval does not automatically reach the people who consumed the disinformation, as they are located in communicative bubble-spaces that are immune to these processes. Verification neither acts on the ecosystem in which disinformation is disseminated, nor does it serve to act at source against those responsible for its creation and dissemination. It is therefore a partial and very incomplete tool.

Acting on the digital ecosystem requires well-honed legal capacities. Hence the importance of the DSA. However, acting at source is much more complicated because while the EU adopts a defensive, legalistic, and protective position, trying to establish attribution processes based on empirical evidence and the use of legal instruments (police, prosecutors, judges, and courts), the actors that develop influence strategies act offensively, strategically and in the long term according to a logic of power and conflict that in many cases is analogous to that of warfare. As RT's director Margarita Simonyan revealed, Russia's networks of influence and interference are not spontaneous: over the last few years Moscow has developed a long-term strategy that has led it to create, cultivate and build loyalty among audiences in the West that could be mobilised at critical moments to defend its positions, weaken the Western consensus, and delegitimise its messages and institutions[8]. Such a long-term media strategy, including TV channels, digital and social media, is something the EU lacks (and which is hardly available to a government apparatus in a democratic society). Thus, in its fight against the abuse of technology to undermine democracies, the EU is doubly hamstrung by a defensive and legalistic logic that prevents it from acting proactively and in accordance with a geopolitical and security logic. What can it do about this and what is it doing?

A digital Bretton Woods

As a result of reflection on the EU's insufficient external activism in digital matters, and concerned about both the growing intersection between geopolitics and technology and the rise of digital authoritarianism, in July 2022 the EU adopted its first external digital[9]. This strategy sets out for the first time the need for the technological and digital component to be a central element of the EU's external action and, at the same time, aims to combine and coordinate under a single strategy element of political action that have hitherto been scattered, such as the external action aspects of the cybersecurity strategy, the action plan on democracy or the fight against hybrid threats, including foreign information manipulation and interference (FIMI).

In addition to this coordination vocation, the Council invited the Commission and the High Representative to work closely with like-minded countries, both bilaterally and regionally and in the field of multilateral organisations to maintain an open, free, global, stable, and secure Internet based on a multi-stakeholder approach. In doing so, the EU consolidates its vocation to influence the global governance of technology. All of this with the aim of imprinting on this governance its humanist and rights-based vision of technology or, as the Council points out, with the aim of influencing the shaping of "ethical, safe and inclusive international technology standards". Special attention should be paid to the expression of the will to act on "countries of strategic importance that have a high level of vulnerability" as well as to combat Internet shutdowns, arbitrary or indiscriminate digital surveillance and data retention, protect human rights defenders and civil society online and expand civic spaces.

This is an ambitious agenda which requires coordination between multiple levels, both within the Commission and between the European institutions, and in turn between them and the member states. Just as important, if not more so, is that such a strategy requires close and in-depth dialogue with third actors, both bilaterally and multilaterally. Some of these, such as the Trade and Technology Council (TTC) with the United States, or the digital partnerships with Japan, Canada, or Korea, are already underway. The EU has also shown its vocation to coordinate its strategies with Indo-Pacific countries, the African Union, and Latin America, as well as renewing its cooperation in the framework of organisations such as UNESCO, the ITU and the OECD.

However, if the EU is to become this "force for digital good", it will have to go much further. As has been said many times, the weight, power, and attractiveness of its internal market tends to turn the EU into a regulatory superpower. The accumulation of legislation on digital and technological matters approved by the EU in recent years, which covers everything from data to artificial intelligence, digital markets and services or cybersecurity, undoubtedly makes the EU the most densely regulated digital and technological space in the world and, of course, a benchmark for many countries (not least the very same US) to imitate.

Ideally, with all these regulations in place, and with its successful implementation, the EU would be in a position to claim to have achieved its desired goal of strategic autonomy (or, at least in part, 'digital sovereignty'). With respect to the rest of the world, it could rely on the so-called 'Brussels effect' popularised by the conversion of its European data regulation (GDPR) into the global data gold standard. But would that be enough? Or credible? As with security, in a global market and in such a conflict-ridden geopolitical environment, the risks and threats posed by technology are not divisible. As in so many other matters, even if it could, the EU cannot aspire to standards so high that by their very cost and nature they are unattainable by the rest of the world. The “Galapagos effect”, by which the EU would be so advanced in its rules that it could not relate or deal with anyone, is simply not possible or desirable[10]. The EU must therefore think in terms of global governance. This requires seeking to empower third parties, be they governments, parliaments, independent institutions, civil society, or experts outside Europe.

One of the great difficulties in this task is the relationship with the US. In a world dominated by geopolitical rivalries and high-voltage tensions between the West on the one hand, and China and Russia on the other, there is not enough room for two models of digital governance as opposed to each other as the European and the US. In an ideal world, the US and the EU should be able, together with other like-minded OECD and global south countries, to design a digital governance architecture equivalent of what the Bretton Woods system achieved after World War II. If back then an international liberal order was tailored to merge and satisfy both the material needs and the moral aspirations of liberal democracies, the challenge today would be to achieve a multilateral digital liberal order compatible with liberal values, or at least, given that China and Russia would refuse to be part of such an order, as broad a sphere of rights-based technological governance as possible.

It is clear to no one that the challenge of such a task is enormous. At the core, such as the US, polarisation precludes Washington becoming a driving pillar of such rules-based global governance. And even if legislation matching the EU was approved by the Democrats or through bipartisan agreements, uncertainty about the reversibility of any international agreements the US might eventually commit itself would be very high. Although many domestic actors in the US (states, cities, civil society) aspire to this regulatory convergence with the EU that could eventually become a template that could be extended globally, the difficulty of reaching bi-partisan consensus and the classic reluctance of the executive and legislative branches to reach internationally binding agreements make it very difficult to unblock this first step. For this reason, although agreement between the US-EU is not a sufficient condition for global governance, it is a necessary one.

Beyond transatlantic tensions, there is a plethora of actors in the global south and the G-20 orbit (India, Brazil and others) whose cooperation and contribution are essential. For both the US and the EU, talking and agreeing with them is extremely difficult. And not so much because their alignment with democratic and liberal values is weak or fragile (where are they not nowadays?: as it is said, “let he who is blameless cast the first stone”) but because their vision of international order and global governance is mediated by their past negative experiences with the West. To the extent that, not without reason, many of these countries conceive the multilateral order as a purely Western artifact aimed at safeguarding Western power and excluding others, their participation in such an enterprise cannot be taken for granted: on the contrary.

Conclusions

Convergence among democracies must come from below, not from above. Not by the talk, but by the walk, so that countries see the tangible benefits of such a model and make it their own, out of pure selfishness. Just as after the Second World War, the US and the other liberal democracies managed to fit their economic and security interests into a multilateral framework that was also liberal, the challenge for the EU today is to offer liberal democracies a similar model of embedded multilateralism in terms of global internet governance. As a matter of both interest and principle, the EU's DNA demands the same approach to the governance of technology that health or the environment: as a global public good to the provision of which it contributes decisively, even if unilaterally at the beginning to unlock a tit-for-tat model of cooperation. Just as God can write straight with crooked lines, the EU can unilaterally promote technological governance in the interest of all by going solo at the beginning and then invite others in to to try and set up a multilateral framework regulating digital technologies for the benefit of all.

Endnotes

[1] Freedom House. (2023). Freedom in the World 2023: Making 50 years in the struggle for democracy https://freedomhouse.org/sites/default/files/2023-03/FIW_World_2023_DigtalPDF.pdf

[2] European Council on Foreign Relations. (n.d.). Power Atlas: Culture, https://ecfr.eu/special/power-atlas/culture/#weaponising-the-vulnerabilities-of-other-systems-rather-than-being-a-city-on-a-hill

[3] Freedom House. (2022). Freedom on the Net 2022: Countering the Authoritarian Overhaul of the Internet, https://freedomhouse.org/report/freedom-net/2022/countering-authoritarian-overhaul-internet

[4] Australian Strategic Policy Institute. (n.d.). Cyber-enabled foreign interference in elections and referendums, https://www.aspi.org.au/report/cyber-enabled-foreign-interference-elections-and-referendums

[5] Facebook. (2021). IO Threat Report May 20, 2021, https://about.fb.com/wp-content/uploads/2021/05/IO-Threat-Report-May-20-2021.pdf

[6] European External Action Service. (n.d.). G20: Difficult times for multilateralism, https://www.eeas.europa.eu/eeas/g20-difficult-times-multilateralism_en

[7] European External Action Service. (2022). EU Ambassadors Annual Conference 2022: Opening speech by High Representative Josep Borrell, https://www.eeas.europa.eu/eeas/eu-ambassadors-annual-conference-2022-opening-speech-high-representative-josep-borrell_en

[8] EUvsDisinfo. (2018). Chief Editor: RT is Like "a Defence Ministry", https://euvsdisinfo.eu/chief-editor-rt-is-like-a-defence-ministry/

[9] Council of the European Union. (2022). ST 11406 2022 INIT, https://data.consilium.europa.eu/doc/document/ST-11406-2022-INIT/en/pdf

[10] *idem.*

6. Re-balancing power to ensure digital rights in the Global South.
Maria Paz Canales

Abstract

Technology policy like any other field of policy is an exercise of power dynamics by different stakeholders that is far from neutral about ideas of order and society building. The policies involved in the development and deployment of technologies and the norms that guide them demonstrate the influence of geopolitical tensions on the lens of what constitutes roles in production, control, and benefit between the Global South and Global North stakeholders.

This essay calls attention to a few areas in technology policy that could benefit from new ways of engagement to re-balance the relationship between north and south and ensure the protection of digital rights across the globe. "Global South" here refers to any stakeholder coming from less developed countries, in majority, but not exclusively, located in the southern hemisphere. Some academics have proposed a shift in the language to reflect that most inhabitants of our planet are located in those jurisdictions.[1]

Data flows from the Global South, but who controls the technology?

The collection and use of data has a political economy behind it. The narrative of trusted frames for facilitating data flow so often present in trade negotiations, in the Organisation for Economic Co-operation and Development (OECD) strategies, and in World Economic Forum (WEF) work is carefully crafted to ensure the extraction of economic value on data as key elements for innovation, economic growth, and development.

Personal data is intrinsically linked to self-determination and to human dignity. But nowadays, personal data is used extensively for the personalization of products, information access, and experiences. Personalization is not only a driver of our consumer behavior, but also the filter of our perception of the world around us that contributse to the creation of our social and political views. And personalization will become increasingly important as we move toward connected bodies and spaces, like medical and wellbeing devices, smart cities and homes, and AR and VR social engagement spaces.

A fully personalized environment thanks to the data collected about human experiences poses important questions around autonomy and the rules of subtle manipulation. Heretofore, the control of the collection and use of personal data during the digital age has been concentrated in private companies predominantly from the Global North that have created and control the technologies through which data is collected and economically exploited as the base of their business model, a sector referred to as "surveillance capitalism."[2]

As pointed out by IT for Change, the Global South represents a major source of the human-generated data. Yet, the societies of the Global South feeding the international data flow have not received equitable economic benefits and meaningful protections from powerful platforms and tools largely controlled by corporations based in the Global North.[3]

To illustrate this trend, let us take as study case AI systems' development and deployment.[4] The proliferation of AI systems in the Global South have taken place under business models of development preferentially exploited by companies from the Global North. The strong asymmetry in data governance between developed countries and the Global South represents a central political and economic challenge because developing countries are generators of data, but not producers of solutions nor able to effectively police a use of data respectful of human rights.

The political economy appears clearly here when many governments from the Global South fell into the trap of the technology race. In Latin America, for example, several countries have proposed national AI strategies to position themselves as leaders in the region,[5] but they have lost sight of how implementations might impact on quality of life and exercise of rights of their citizens, particularly vulnerable groups.[6]

Visions most often focus on the economic value of the implementation of AI and reference the concepts of digital transformation and the fourth industrial revolution borrowed from the WEF and the OECD. This is how the States appear as the facilitators of a market and primary clients for AI systems. Rather than mapping societal needs that could effectively be addressed using technology, their efforts start with mapping the industry and the employment capacities and infrastructure necessary to create a local AI market. Little attention paid to enhancing regulatory capabilities or readiness assessments of institutional frameworks.

This trend is fed and welcomed by technology providers in the Global North who are eager and able to offer their technologies in these emerging markets and reap the benefits of huge contracts and the feedback loops of knowledge for improving their technologies through a massive collection of data under limited or inexistent regulatory oversight.

What many refer to as the "AI gap" describes how those who have the ability to design and implement AI applications configure a technological development that is opaque to the majority of citizens. Gasser and Almeida propose a model to address the governance of AI based on the consideration of three challenges: informational asymmetries; the need and difficulty of generating a normative consensus; and the governance mechanisms.[7]

"Information asymmetries" refers to the concentration of knowledge about the basic technologies that support AI in a few experts, most often residing in the Global North. The consequence of this concentration of expertise is a relevant gap between users, decision-makers, and technology developers/owners. A primary objective of a governance system should therefore be to develop mechanisms that promote a more widespread understanding of AI and its applications in society.

The second challenge, namely reaching a normative consensus, highlights not only the risks and challenges of AI, but also its potential benefits for humanity, including the sustainable development goals (SDGs). In this sense, a future AI governance model should address the current preparation of regulatory frameworks, the expectations of different sectors, and the interoperability between frameworks.

To ensure that the societies of the Global South countries can benefit from technology in a more balanced way, we must urgently reframe the socio-political component of its deployment. More should be done in terms of national capacities that incorporate data infrastructure, data commons access, competencies for the management of data, and regulation to ensure technology deployment consistent with the exercise of human rights. This last point requires considering as pre-requisite of emerging technologies' deployment by implementing basic regulations for the protection of personal data, open data collection, and non-discrimination.

To better balance the benefits with the risks of technology deployment, governance mechanisms should be part of the roadmap of technology deployment in the Global South. This critically includes a more participative approach and the engagement of those who control the technology, whether private or public actors, with the communities that will be impacted by the technology. The UN Guiding Principles on Business and Human Rights (UNGP) provide an interesting opportunity to anchor this business responsibility approach for technology provision within the framework of human rights protection, respect, and remedy.

This strategy aims not to undermine the value of the contribution from the private sector that predominantly holds the power on technology development today. It looks at re-balancing the current relationship with a geopolitical perspective that allows for a fairer distribution of the benefits of technology, respects the human rights of the populations of the Global South, and departs from the current dynamic of treating the region as a field for experimentation on human subjects without their informed consent.

What is the role of international cooperation in the promotion of human development through technology?

Even when cooperation is motivated by altruistic values to collaborate with the leapfrogging of developing countries in the Global South, usually with the tagline "technology for good", developed countries and their companies set the priorities, including the model for economic development. Cooperation should find a way to better connect and provide technical support to allow developing countries to define the role of the cooperation with their own strategies, including their poverty reduction and SDGs accomplishing strategies.

Civil society groups have witnessed with concern over recent years many such initiatives as biometric identification systems, predictive criminal systems, electronic voting, facial recognition in public spaces and borders, digital welfare, digital health that are promoted and financed through international cooperation. These initiatives stimulate the development and incorporation of technologies in public policy to improve a state's efficiency without a comprehensive assessment of their impact on the exercise of such human rights as privacy, freedom of expression, the right to peaceful assembly, and the right not to be discriminated against.

The private sector often holds a relevant interest in the cooperation programs to advance in the opening of new markets for their technologies. In these cases, the relationship with international cooperation bodies and their efforts should be a lot more transparent about how technical cooperation engagement with private companies take place and how this engagement influences their decision-making process about the promotion of specific technologies as part of these cooperation programs. Responsible cooperation aligned with SDGs requires that investment decision-making in the development and implementation of such technologies be transparent, participatory, and supported by evidence supported as much as possible to ensure their legitimacy and consistency with democratic values.[8] More attention should be given to the implementation of effective multi-stakeholder participation in any international cooperation engagement in order to balance the influence of private sector in the international cooperation decision-making processes.

A particularly useful study case to illustrate the role of international cooperation in technology deployment in the Global South is the implementation of digital identity systems. Most of the initiatives are portrayed as an opportunity for the achievement of social and economic rights through digital government services like welfare, health, and public safety. The World Bank's Identification for Development (ID4D) initiative has globally championed and financially supported a digital ID model driving consensus toward an 'identification for development' concept. As has been extensively reported by the Center for Human Rights and Global Justice of the New York University School of Law,[9] the popularity of these systems in the Global South reflects the expectation that they can contribute to inclusive and sustainable development and the realization of human rights. But the ID systems that the World Bank supports are heavily infused with a 'transactional' or 'economic' identity approach. Behind them lay the promise of a 'single window' that will allow each individual to transact with both government and private sector actors, improving access to public and private services, and therefore creating digital economies and fueling economic growth. More often than not, these systems are inadequately equipped to deal with difficult questions about the legal status of marginalized or vulnerable groups and their access to the system. Digital ID systems deployed under this paradigm exacerbate pre-existing forms of exclusion and discrimination in public and private services:

"The use of new technologies may lead to new forms of harm, including biometric exclusion, discrimination, and the many harms associated with surveillance capitalism. Meanwhile, the promised benefits of such systems have not been convincingly proven."[10]

As this landmark example demonstrates, international cooperation has been key to stimulating the creation of a market for technologies around the globe, but it could play an even more fundamental role in ensuring the provision of transparent and democratic technologies that are committed to respect human rights. Thus, investment in technologies must be accompanied by requirements that public and private entities that are recipients of international cooperation funds define clear and specific regulatory frameworks for the conditions of use of such technologies in a manner compatible with the exercise of human rights and go beyond the minimum legal requirement in some countries with less regulatory development in these matters to ensure that mechanisms of independent control, transparency, and accountability to citizens impacted are in place for those technologies.

Guidelines for the development of selection criteria for technology providers that conform to a standard of probity and unrestricted commitment to human rights could also be formulated from the mechanisms of international cooperation. A human rights impact assessment requirement as pre-requisite for funding and support from international cooperation entities for technology deployment projects would advance this goal.

Last but not least, there is a relevant role for international cooperation in the mainstreaming of gender intersectional considerations in the promotion of technology deployment. Technology deployment has insufficiently focused their design and evaluation on the differential impacts that they can have on marginalized and vulnerable populations. The predominant business models do not account sufficiently for gender equality and the needs of special protection groups, so any technological implementation made under using this same logic of implementations will fail to properly account for a gender intersectional approach.[11]

The core of the international cooperation mission should be evaluation of the differential impacts and risks to traditionally marginalized or vulnerable groups, among them women and gender diverse populations, in the deployment of data-driven technology implementations. Why is this particularly relevant in re-balancing power to ensure exercise of human rights in the Global South? Because structural inequalities related to gender and their intersectional implications are part of the institutional challenges that the countries of the Global South countries are attempting to be address with the use of technology. To succeed in that goal rather than risk replicating and escalating gender inequality, technology deployment promoted by the international cooperation needs to put gender at the center.

Who participates in the setting of global norms and the oversight of the promotion of human-rights-respecting technologies?

When we observe the current global regulatory trends, we identify a flourishing enthusiasm in technology regulation that is far from the hands-off approach that characterized the emergence of those technologies. This approach is still rather geographically fragmented, and jurisdictions in the Global North are considerably more nuanced in their analysis.

There is no absence of agreement, however, on the core human values in current human rights international instruments that are equally applicable to new and emerging technologies. The balancing test of legality, necessity, and proportionality that have been part of the international human rights standards developed over the last fifty years can continue to be a useful tool to measure and weigh the pertinence of new and emerging technologies.

Emphasis on innovation has tinted the discussion about global technology regulations with the perception that the problem must be addressed from ethics or regulatory sandboxes. Ethical considerations will be always helpful as complements and best practices, but the impact of technology deployment on rights should move the norms setting discussion to how to better implement protections rather than assuming the absence of protection of human rights in face of technology uses.

Although the Global South continuously struggles to ensure the effective exercise of human rights, there is no shortage of recognition for international instruments that protect them. To uncouple the conversation about technology regulation from those already well-established standards and present it as an entire new field risks limiting the debate to technical and economic aspects. We ought not exclude proper consideration for a human impact approach when identifying the risks to and opportunities for human rights at the core of the regulation. It also implies limiting the discussion to technology experts and excluding the rich experiences of human rights institutions and human rights defenders who play a fundamental role in promoting the rights of traditionally marginalized or vulnerable groups in the Global South.

In recent years, an effective way to operationalize human rights international rules has gained traction by promoting human rights due diligence throughout the entire life cycle of new and emerging technologies. There are currently no consistent practices among public or private entities to conduct human rights impact assessments as part of the design and deployment of technologies. But there is a fundamental opportunity to leverage the last ten years' experience and the normative force of the UNGP to look for ways to strengthen their implementation and create mechanisms of enforcement.

As pointed out in the first section of this essay, the control of technology rests primarily with those who build it in the Global North. Consequently, they have built the rules of use of for those technologies usually clamoring for the exclusion of state action, and in this way disputing (or even eroding) its institutional power.[12] Global south actors have been doubly absent from this process: they are not producers of technology, do not have the capacity or willingness to regulate technologies, and are always afraid of the negative impact of their regulatory action on innovation and economic development.

Today, the significant number of Global North countries and regional blocks start to be active in technology regulation, and this raises a question about the role of Global South actors will take, whether they be governments, companies, or civil society in general, in the creation of rules that will have global impact. The "Brussels effect,"[13] a term coined to describe the expansive impact of the regulatory action of the EU beyond European countries, proposes that such recent EU regulations as the Digital Market Act (DMA), the Digital Service Act (DSA) and the Artificial Intelligence Act (AI Act) will influence how technology companies function. How will those regulations impact regulations in global south markets?[14] On the same line, those regulations are a source of inspiration and sometimes even boilerplate for other governments.

Elsewhere, we see international bodies sprinting to provide regulatory guidance for the extended world, with differential consequences for Global South actors more willing and more reliant on expert advice given their capacity shortage in some of these complex issues. Here, we can take as a study case the most recent UNESCO proposal to develop a "Guidance for regulating digital platforms."[15] The goal is laudable: provide guidance to Member States' regulatory efforts and ensure regulatory coherence. This objective, however, can be better fulfilled through principles that can be implemented in a flexible way to adapt to the normative and institutional conditions of the countries in which they will be implemented. The vocation for universality of the proposal places restrictions ob the institutional capacity of the states. The different normative traditions for the protection of freedom of expression must be respected in the development of the proposed regulation.

The process was supported at the beginning by a handful of experts who were closely selected to advice. Broader information for meaningful engagement of multi-stakeholders' groups and experts from the Global South only occurred at the later stages. Regrettably, this is only one example among many of how the engagement of Global South multi-stakeholder actors, particularly civil society, in technology global norm setting seems an afterthought rather than priority for international bodies. This at the forefront of concerns today when new international oversight bodies to oversight artificial intelligence are under discussion.[16] Whatever the form of international governance taken forward, it is imperative that it is not shaped not only by Global North leadership, but also by the active engagement of the societies in which AI is being promoted by companies and economic development institutions as tools to help to overcome structural inequalities, improve access to services, and provide economic development. Deployed without a thorough social diagnosis of where and how AI can be a concrete and efficient contribution to achieving those goals and avoid risks for the exercise of human rights is crucial.

Finally, a much less attended but equally salient issue in ensuring the respect of digital rights is how Global South actors can participate in or build their own mechanisms for the oversight of technology regulation arising at global level. This leads us to explore how the compliance with human rights of private companies' commitments that come from their own policies can be enforced from the perspective of global south actors through such mechanisms as transparency reports, voluntary external auditing, independent voluntary oversight,[17] and multistakeholder accountability mechanisms.[18] It is also worth asking what the role of Global South users in the enforcement of the legal standards created elsewhere to avoid discrimination in the provision of services by global companies could be.

Agustina del Campo has argued that oversight should be at the center stage of technology regulatory debates for three reasons: "1) it forces us to think and clearly state the objectives of the regulation (what we want to see happening and why); 2) it allows us to test the means to our ends; 3) it helps clarify the trade-offs that the substantive regulation proposes."[19] Applying this proposed structure to the Global South regulatory efforts could be a mindful strategy to allocate always scarce resources.

There is no shortage of challenges to identifying oversight mechanisms to ensure the respect of human rights in the use of technology that will be effective for the Global South. Probably the thorniest problem is the legitimacy of voluntary mechanisms, whether they are designed by self-regulation from private companies or as part of the co-regulatory efforts from states. In all cases, ensuring independence seems as critical as ensuring the resources for their effectiveness. Another relevant issue is the interaction of this mechanism with local judicial enforcement and the supervision of cross-jurisdictional behaviors across legal traditions and institutional realities.

To address all these challenges, a robust participation of stakeholders from the Global South is necessary at early stage in the design of regulatory frameworks with the potential for global influence. Since there are not many governments, civil society organizations, research institutions, or even companies from the Global South with the financial and human resources to run research programs on tech regulation or engage effectively in regulatory process happening at global level, there is an increased need to invest in the full spectrum of skills needed to support a global south participation that can be independent and effective in representing the diversity of stakeholder visions.

Conclusion

The increasing role that technology plays in every aspect of social interaction makes democracy and the rule of law heavily dependent on the ability of the Global South's citizens to ensure the legitimacy of technology deployments that impact the exercise of their rights and shape their present and future development.

This is a rather socio-political debate that requires that how private corporation design technologies, how international cooperation promotes technologies, and how technology norms are set take into consideration the specific needs of the Global South populations, the diversity of their institutional and legal frameworks, and their cultural differences to frame technologies such that they ensure the exercise of human rights and break free from a colonialist pattern.

The Global South should no longer be regarded as the field of experimentation and a data source and participate in a more globally balanced technology policy shaped to deliver the technological benefits and avoid worsening local and geopolitical inequalities.

Endnotes

1 Alam, Shahidul (2008). Majority World: Challenging the West's Rhetoric of Democracy, Amerasia Journal, 34:1, 88-98.

2 See Zuboff, Shoshana (2017). The Age of Surveillance Capitalism. New York: PublicAffairs.

3 Gurumurthy, Anita et al (2022). Beyond the North-South Fork on the Road to AI Governance: An Action Plan for Democratic & Distributive Integrity. Initiate: Digital Rights in Society - Paris Peace Forum. Available at: http://www.digitalrights.ai/report

4 Derechos Digitales have conducted Artificial Intelligence implementation research in Latin America examining its impact in inclusion. See https://ia.derechosdigitales.org/

5 Aguerre, Carolina (2020). Estrategias nacionales de IA y gobernanza de datos en la región. En C. Aguerre, (Ed.). Inteligencia Artificial en América Latina y el Caribe. Ética, Gobernanza y Políticas. Buenos Aires: CETyS Universidad de San Andrés.

https://guia.ai/wp-content/uploads/2020/05/Aguerre-Estrategias-nacionales-de-IA-y-gobernanza-de-datos-en-la-region.pdf

6 Velasco, Patricio & Venturini, Jamila (2021). Automated decision-making in public administration in Latin America. A comparative approach to its application in Brazil, Chile, Colombia and Uruguay, Derechos Digitales. Available at: https://ia.derechosdigitales.org/wp-content/uploads/2022/03/09_Informe-Comparado-EN_180222_compressed.pdf

7 Gasser, Urs, and Virgilio A.F. Almeida (2017). A Layered Model for AI Governance. IEEE Internet Computing 21 (6) (November): 58–62 https://dash.harvard.edu/bitstream/handle/1/34390353/w6gov-18-LATEX.pdf?sequence=1

8 See the Digital Rights Check, a human rights assessment tool and guidance meant for staff and partners working in technical development cooperation and in development finance, who are working on digital projects or are otherwise using digital solutions. Available at: https://digitalrights-check.bmz-digital.global/

9 Center for Human Rights and Global Justice (2022). Paving a Digital Road to Hell? A Primer on the Role of the World Bank and Global Networks in Promoting Digital ID, New York University School of Law. Available at: https://chrgj.org/wp-content/uploads/2022/06/Report_Paving-a-Digital-Road-to-Hell.pdf

10 Ibid.

11 Canales, Maria Paz and Venturini, Jamila (2022). A Feminist Lead Towards an Alternative Digital Future for Latin America, Bot Populi. Available at: https://botpopuli.net/a-feminist-lead-towards-an-alternative-digital-future-for-latin-america/

12 See Zuboff, Shoshana (2022). Surveillance Capitalism or Democracy? The Death Match of Institutional Orders and the Politics of Knowledge in Our Information Civilization, Organization Theory, Volume 3: 1–79. Available at: https://journals.sagepub.com/doi/epdf/10.1177/26317877221129290

[13] Bradford, Anu (2020). The Brussels Effect: How the European Union Rules the World, Faculty Books. 232. Available at: https://scholarship.law.columbia.edu/books/232

[14] As stated by Torreblanca supra. p.49: "The EU must therefore think in terms of global governance. This requires seeking to empower third parties, be they governments, parliaments, independent institutions, civil society, or experts outside Europe".

[15] UNESCO. Guidelines for Regulating Digital Platforms for Information as a Public Good. Available at: https://www.unesco.org/en/internet-conference/guidelines

[16] See Bak-Coleman, Joseph et al (2023). Create an IPCC-like body to harness benefits and combat harms of digital tech, Nature, Vol 617. Available at: https://www.nature.com/articles/d41586-023-01606-9; Park, Y.J. (2023) How we can create the global agreement on generative AI bias: lessons from climate justice. AI & Soc, available at: https://doi.org/10.1007/s00146-023-01679-0; Hogarth, Ian (2023). We must slow down the race to God-like AI, Financial Times. Available at: https://on.ft.com/3LeOkan

[17] See Oversight Board for Facebook. Available at: https://www.oversightboard.com/

[18] See Global Network Initiative. Available at : https://globalnetworkinitiative.org/

[19] Del Campo, Agustina (2022). Platform Oversight: A Neglected Link in Internet's Regulatory Futures, Center for Studies on Freedom of Expression and Access to Information (CELE) at Universidad de Palermo, Argentina. Available at: https://www.palermo.edu/Archivos_content/2022/cele/noviembre/paper-cele/Platform-Oversight.pdf

7. Digital Democracy in Asia.

Trisha Ray

Abstract

A pain point preventing some Asian countries from participating actively in discussions shaping digital democracy is the Eurocentric, Americentric perspective on what the "correct" practice of democracy should be. This article conducts a review of literature on digital democracy from Asia, covering how digital technologies have improved government service delivery, enhanced transparency, enabled wider political participation, and provided spaces for underrepresented voices. It also finds nuance in how different Asian publics – including within the same country – are engaging with politics online, with its practice varying based on history, cultures, political systems, and communities. For instance, even with the focus on developing e-government infrastructure across Asia, not all communities experience these services in the same way, resulting in a 'democratic divide'.

Introduction

Technologies reflect the societies that use them, and in turn shape societies in their image. "Digital democracy" then is not just about the use of digital technologies to promote democracy, but about how the tools themselves are shaping our societies. In recent years, as open societies are confronted with both the promise and perils of online platforms, this relationship has been condensed into a two-part question, highlighted in the introductory essay by Irene Blasquez-Navarro: can democracies survive digital technologies? Can they survive without them? One such ouroboros-like relationship is that between digital tech and the public sphere. The democratization of access, which provides the average citizen a pulpit to voice their views, unmediated, seemed to be the ultimate realization of Habermas' undistorted public sphere. The same access and (relative) affordability transformed these same platforms into echo chambers reflecting narrow, even harmful interests. How do we ensure that the geopolitical aspects of digital democracy do not come at the cost of creating echo chambers about what the "right" model looks like? In my paper with Jan Hornat for the 2021 Forum 2000, we highlighted one critical challenge: research and, by extension, agenda-setting power on digital democracy is concentrated in a handful of Atlantic countries.[1] The countries of Asia, each with their distinct political systems, peoples, and histories, therefore capture a variety of relationships between publics, governments, and online spaces.

This essay analyzes 25 papers on digital democracy, published between 2015 and 2022, focusing on East, Southeast and South Asia, and parses common themes stemming from their literature. Asia is home to some of the most rapidly growing online populations in the world: the people in its subregions are spending more time online, with larger portions of their lives being conducted in digital spaces, including forging social connections, e-commerce and entertainment, as well as politics and governance.

Table 1: Internet penetration rate (2014 vs. 2020) of selected countries in Asia[2]

Country	Internet users (% of population) 2014	Internet users (% of population) 2020

China	48	70
Japan	89	90
South Korea	88	97
Indonesia	17	54
Malaysia	64	90
Philippines	35	50
Singapore	82	92
Thailand	35	78
Vietnam	41	70
Bangladesh	12	25
India	14	43
Pakistan	10	25
Sri Lanka	11	35

Although internet connectivity varies considerably, with internet penetration ranging from a quarter of the population, up to nearly 100%, the sheer size of Asia’s population means that even relatively “unconnected” populations still translate into large numbers. For instance, in 2020, of the 3.5 billion people online, 990 million were from South Asia.[3]

Digital democracy has been used to describe, at one level, the use of information and communication technology (ICT) to enhance democratic governance and citizen participation in democratic processes: “E-Democracy refers to the processes and structures that encompass all forms of electronic interaction between the Government (elected) and the citizen (electorate)”.[4] Others have defined it as “the collection of attempts to practice democracy without the limits of time, space, and other physical conditions, using ICT or CMC instead, as an addition, not a replacement for traditional ‘analogue’ political practices”.[5] In other words, digital democracy is not just about how governments engage with citizens, but also a wider gamut of democratic features, such as a vibrant public sphere, and an active and politically-engaged citizenry.

More recently, digital democracy is often defined in opposition to digital authoritarianism, a model of the internet that “allows states to censor online speech on arbitrary grounds, using nebulous justifications like national security and social harmony. It also enables widespread surveillance and control of citizens.”[6] However, such a dichotomy supposes that democratic governments do not have “authoritarian” compulsions, and that democratic expression cannot exist under authoritarian regimes. At the 2021 Summit for Democracy, USAID Administrator Samantha Power stated that, “The abuse of technology and personal data to spread disinformation, to surveil citizens and violate their rights and to pit citizens against one another are problems that can start at our shores.”[7]In this volume as well, Jeremy Cliffe aptly notes, “the focus should be…on bottom-up methods of encouraging democracy rather than top-down impositions, and on the underestimated art of persuasion rather than a them-and-us approach”.

As mentioned earlier, the pasts and politics of each country are unique, presenting both challenges to the practice of digital democracy, and windows into the myriad ways in which digital democracy can be expressed. In Malaysia, for instance, "Despite early attempts to establish ideologically-based parties, the default mode of operation returned to racial identities…This was further reified by the establishment of the first ruling coalition represented by three major race-based parties set up under the pretext of ensuring the wellbeing of the major races of Peninsular Malaysia (the Malays, Chinese and Indians). This coalition, that would become known as Barisan Nasional (National Front), was in power for over 60 years before it was toppled in the GE14 by Pakatan Harapan that took over on 8 May 2018."[8] This background implicates the policies, rules, systems, and algorithms of social media platforms and how they are used in political processes.

How Asia Sees Digital Democracy

Digitally Transforming People's Lives

The most foundational way in which technologies aid democracy is through transparent, accountable and accessible government services. Indeed, as mentioned in the framing for this section, the early definitions of digital democracy were synonymous with e-government. E-government includes a panoply of uses of ICT to ease citizen engagement with government and enhance government operations, from e-registration of voters and provision of information on political candidates, to platforms that make it easier for residents and citizens to access social security and other critical services.

Many countries of Asia have undertaken measures to modernize governance, and the COVID-19 pandemic has provided an added impetus to digitize services. E-government readiness does, however, vary from country-to-country, depending on availability of capital, development of connectivity infrastructure, accessibility and cost of devices and services, among other factors.

Table 2: E-Government Development Index (EGDI) Rankings (2016 vs. 2022) of selected countries in Asia.[9]

Country	EGDI Rank (2016)	EGDI Rank (2022)
China	63	43
Japan	11	14
South Korea	3	3
Indonesia	116	77
Malaysia	60	53
Philippines	71	89
Singapore	4	12
Thailand	77	55
Vietnam	88	86
Bangladesh	124	111
India	107	105

Pakistan	159	150
Sri Lanka	79	95

The transformation of government service delivery through digital innovation is a recurrent theme in literature covering South Asia, a focus that is not wholly surprising given the immense demographic pressures in this sub-region. In 2020, South Asia accounted for nearly a quarter of the world's population, a figure likely to grow with India having overtaken China in April 2023 as the world's most populous country.[10] The region must also overcome development challenges, including education and skilling for this growing population, healthcare, empowering women economically, among other social-structural issues. In a bid to address these challenges through a digital-led approach India has, for instance, successfully deployed Digital Public Infrastructure (DPI), foundational infrastructure built for public good that "mediates the flow of people, money and information".[10] This includes a foundational biometric ID, a unified payments interface for seamless payments, and the ability to store, transmit and authenticate documents digitally for access to services. Bangladesh, India, Pakistan and Sri Lanka all have digital transformation policies, predicated on techno-legal approaches that purport to ensure that benefits accrue to all.[12]

"However," as a World Bank report notes, "apart from India, innovation ecosystems in other South Asian countries are nascent".[11]

Furthermore, the intersection of development challenges with pervasive social stratification has rendered the promise of e-democracy far from complete. There are several levels to the exclusion of communities from e-government: access to hardware, such as mobile phones or computers; skills and education needed to be able to engage meaningfully with these services; trust in e-government tools; and historical social divides, such as those based on ethnicity, gender, religion and race.[13]

One article on the experience of migrants in South Korea hypothesizes that the socio-political context in which systems are built exclude groups by design, implicitly if not explicitly:[14] "[Several] government websites are devoted to migrants...However, this increase in the number of websites devoted to services for migrants did not necessarily enable service needs to be met or reduce barriers to access, as they were not designed with a migrant user in mind." Similarly, an article on Bangladesh's digitalization experience asserts that…"the leap into creating digital infrastructures has also engendered new vulnerabilities and reaffirmed power hierarchies within Bangladeshi society."[15] Thus, even with efforts to improve a country's e-government infrastructure not all communities experience these services in the same way, resulting in a 'democratic divide', the contours of which are unique to each country's history, politics and culture.

"Digital Pitfalls": Access vs. Control over Online Spaces

The initial promise of digital democracy was that the very nature of online spaces – decentralized, borderless – would challenge the dominion of the "weary giants of flesh and steel", the brick-and-mortar institutions that held sway over the physical world. This vision was seemingly actualized during the Arab Spring, which demonstrated the power of online platforms to help mobilize vast swathes of people for a common cause. More recently, an effective opposition, paired with rapid dissemination of alternative information through peer-to-peer media like Whatsapp, was instrumental in regime change in Malaysia in 2018.[16]

Although presence in online spaces has been made easier with the advent and proliferation of cheap smartphones, this has not become a force for democracy in and of itself. A temporary 'democratization' of the public sphere on the grounds of access alone cannot correct institutional problems, such as a weak Fourth Estate and lack of meaningful electoral competition. This phenomenon was highlighted also in Malaysia: "[E]ven if the Malaysians' access to online platforms are unfettered, the platforms are not accessed in the same way, nor do these platforms contain the same meaning for those accessing them due to differences in Internet literacies."[17]

In Bangladesh, restrictions on traditional news media are mirrored in online spheres through heavy-handed government regulation.[18] Concurrently, even when news media is relatively unrestricted, organized troll armies, leveraging social media algorithms, are able to limit the sphere of ideas, swaying public opinion in particular directions. "Online public opinion has been able to enter the offline domain because of the contextual hybridity and the emergence of a hybrid media system. These findings reflect the limitations of public opinion in the digital age."[19] In other words, social media is seen as the arbiter of public opinion, becoming the news source rather than simply a space for discussion. This enables organized groups, including governments, to affect offline opinion and decision making in specific and pernicious ways under the guise of acting on public opinion. In this way, online platforms can help retrench rather than challenge political regimes.[20]

Finally, the question of who defines acceptable speech online remains hotly contested. On the one hand, there is a suspicion of content moderation on platforms, often conducted on the basis of rules and principles shaped by the "West". On the other hand, where rule of law is weak, government-instituted content regulations – such as anti-fake news laws – can be abused by those in power to arbitrarily censor critical or dissenting voices.[21] In Southeast Asia, the harshest controls are over speech criticizing the government, military, judiciary or the royal family (as is the case in Brunei, Cambodia, Malaysia, Thailand). The nature of the internet today allows information to spread quickly and across platforms, limiting state jurisdiction and resulting in governments defaulting to targeting individuals with harsh sentences.[22]

Democracy by Any Other Name: Unconventional Expressions

In the course of scanning papers to select for this paper, civic engagement emerged, by far, as the most frequently-studied theme. Theoretically, social media platforms, blogs and other online "public spaces" that function as platforms for citizens to convene to talk about policies that affect them, and mobilize through both formal (i.e. through established institutions like elections) and informal (protests, petitions etc) channels.[23]

Some studies found that internet access was positively correlated with offline political activism, such as collective petitions, or contacting local governments to express dissatisfaction with policies or government officials.[24] There are caveats to the quality and effects of civic engagement, however. The first is fragmentation. In Singapore, for instance, despite relatively lower infrastructure barriers to participation in online spaces, certain social groups are more active than others, even when internet penetration is high.[25] In that sense, social media is not a true "public sphere" as communities continue to interact in discursive bubbles. Secondly, there is a significant relationship between the type of political system one lives in, the kinds of connections one makes online and their political participation. For instance, one study in East Asia found that young people in China "have more links to activists than those in Hong Kong and Taiwan".[26] Concurrently, internet use in East Asia appears to "decrease electoral and increase activist participation. In an authoritarian context, they indicate a correlation between greater Internet usage and a preference for activist- over electoral-participation".[27] Publics in non-democratic systems often need to get creative in how they express themselves in heavily-monitored/censored online spaces.[28] In 2018, as Chinese censors were battling the country's flourishing #MeToo movement, users began using the rice and bunny emojis, pronounced "mi tu" in Mandarin, to subvert censorship.[29]

Conclusion

Governments fear the destabilizing potential of online platforms in part because our understanding of digital democracy is still limited. There appears to be a growing consensus that the laissez-faire governance model that marked the early years of the internet will not work. At the same time, for any set of principles to become norms, they must be clear and consistent in their application. At the 2021 Summit for Democracy, Forum 2000, the Freedom Online Conference, and other such forums, a recurrent theme has been the absence of a unified model for digital democracy. This paper, by exploring, through a thematic analysis of existing literature, how different governments and publics in Asia are navigating online spaces, sought to nuance the binary framing that is present in our thinking on digital democracy. Three core themes emerged from this discussion.

The first is the use of digital platforms and services to enhance the interface between governments and people. Several countries in the region have, to varying degrees of success, sought to modernize their internal governance processes, build platforms for citizens and residents to find information on and avail government services. Availability does not, however, translate naturally to access, as several country case studies show. Who builds these platforms and how they are used, in addition to their interlinkages with the peculiar politics, histories and social dynamics in the country, result in 'democratic divides'. **The first recommendation is that while there is no single pathway to inclusive digital transformation, it would be worth exploring what has worked in different Asian countries, and how these learnings could be applied in other geographies.**

The second is the tension between unfettered access to social media platforms, and control over what constitutes acceptable speech in these spaces. Several Asian countries have the right to freedom of expression and peaceful assembly encoded in their constitutions, but also have exceptions on the grounds of public safety, national security, defamation and diplomatic relations. Laws like China's Computer Information Network and Internet Security, Protection and Management Regulations (1997), Malaysia's Communications and Multimedia Act (1998), South Korea's National Security Law, Section 112 of the Thai Criminal Code, and blasphemy and sedition laws, all contain such exceptions rooted in specific needs and historical contexts, but with wording that makes them prone to misuse by parties in power. Conversely, heavy-handed control has a chilling effect on the trust and ability of people to use online platforms. In a positive development, UNESCO has released "Guidelines for regulating digital platforms" which recommend principles for platform accountability and the ideal constitution of oversight mechanisms.[30] Platform governance is a global issue with hyperlocal implications: **a second recommendation is the need for independent assessments of the impact of platform controls on livelihoods and quality of life.** Any such new assessment tool must be multi-disciplinary, accounting for the differential impact these technologies will have on people of various genders, ethnicities, socio-economic status etc.

Third, publics in Asia, even those living under repressive regimes, use digital spaces in creative ways to air their aspirations and demands. Civic engagement is therefore the liveliest aspect of digital democracy in Asia and is expressed in atypical ways. How governments and citizens engage with digital technologies and online spaces in Asia falls along a spectrum. Democratic governments display authoritarian tendencies in online spaces, and publics in non-democratic states organize in inventive ways to thwart even the most restrictive government censors.

Endnotes

[1] Trisha Ray and Jan Hornat, “Policy paper: Global Cooperation of Democracies in the Digital Realm”, Forum 2000, October 2021, https://www.forum2000.cz/files/policy-paper-global-cooperation-of-democracies-in-the-digital-realm.pdf

Gonzalez Hernando, Marcos, Williams, Kate, Examining the Link Between Funding and Intellectual Interventions Across Universities and Think Tanks: a Theoretical Framework (International Journal of Politics, Culture, and Society volume 31, pages 193–206, 2018), https://link.springer.com/article/10.1007/s10767-018-9281-2

Clarke Laurie, Williams Oscar, Swindells, How Google quietly funds Europe’s leading tech policy institutes (NewStatesman, 2021), https://www.newstatesman.com/business/sectors/2021/07/how-google-quietly-funds-europe-s-leading-tech-policy-institutes

[2] “Individuals using the internet (% of population), World Bank, ww.data.worldbank.org/indicator/IT.NET.USER.ZS

[3] Shifting Gears: South Asia Economic Focus, Fall 2021”, World Bank, October 7, 2021, www.worldbank.org/en/region/sar/publication/shifting-gears-south-asia-economic-focus-fall-2021

[4] Michiel, Backus. "E-Governance and Developing Countries. Introduction and examples." The Hague: International institute for communication and development (IICD) (2001).

[5] Kenneth L. Hacker and Jan van Dijk, “What is Digital Democracy”, Digital Democracy: Issues of Theory and Practice, (United Kingdom: SAGE Publications, 2000): p. 1.

[6] Trisha Ray and Jan Hornat, “Policy paper: Global Cooperation of Democracies in the Digital Realm”, October 2021.

[7] Summit for Democracy https://www.youtube.com/watch?v=Nw2bfsjTXhA&t=14393s

[8] Clarissa Ai Ling Lee and Eric Kerr, “Trolls at the polls: What cyberharassment, onlne political activism, and baiting algorithms can show us about the rise and fall of Pakatan Harapan (May 2018-February 2020), First Monday, Volume 25, Number 6 - 1 June 2020, https://journals.uic.edu/ojs/index.php/fm/article/download/10704/9551

[9] www.publicadministration.un.org/egovkb/Data-Center

[10] https://www.worldometers.info/world-population/population-by-asia-subregion/ Noore Alam Siddiquee, "E-government and transformation of service delivery in developing countries: The Bangladesh experience and lessons", Transforming Government: People, Process and Policy, Vol. 10 No. 3 (2017): pp. 368-390. https://doi.org/10.1108/TG-09-2015-0039

[11] Sajitha Bashir, Carl Dahlman, Naoto Kanehira and Klaus Tilmes, “The Converging Technology Revolution and Human Capital: Potential Implications for South Asia”, World Bank, 2021.

12 Seo, Jin-Wan and Golam Mehedi. “Where Are E-Governments in South Asian Countries? A Comparative Approach.” South Asian Studies 30 (2015): 7, 01 Jin Wan_30_2.pdf (pu.edu.pk)

13 Nidhi Saxena, “E-Government and E-Democracy: The Role of Technology Vis-A Vis

Indian Socio-Legal Framework”, Cyber Crimes in the 21st Century, (New Delhi, Manakin Press Pvt Ltd: 2017), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2976000

14 Iris Lim, "Exploring Experience at the Intersection of Migration and Digital Democracy in South Korea", Asiascape: Digital Asia 8, 3 (2021): 139-163, doi: https://doi.org/10.1163/22142312-bja10019

15 Abdul Aziz, “Digital Pitfalls: The Politics of Digitalization in Bangladesh”, Communication, Culture & Critique, (2021) doi:10.1093/ccc/tcab037

16 Ross Tapsell, “The Smartphone as the “Weapon of the Weak”: Assessing the Role of Communication Technologies in Malaysia's Regime Change.” Journal of Current Southeast Asian Affairs 37 (2018): 29 - 9.

17 Clarissa Ai Ling Lee and Eric Kerr, “Trolls at the polls: What cyberharassment, onlne political activism, and baiting algorithms can show us about the rise and fall of Pakatan Harapan (May 2018-February 2020), First Monday, Volume 25, Number 6 - 1 June 2020, https://journals.uic.edu/ojs/index.php/fm/article/download/10704/9551

18 Abdul Aziz, “Digital Pitfalls: The Politics of Digitalization in Bangladesh” (2021)

19 Taberez Ahmed Neyazi, “Digital propaganda, political bots and polarized politics in India”, Asian Journal of Communication, 30:1, (2020): 39-57, DOI: 10.1080/01292986.2019.1699938

20 Aim Sinpeng, “Digital media, political authoritarianism, and Internet controls in Southeast Asia”, Media, Culture & Society, 42(1), (2020): 25–39. https://doi.org/10.1177/0163443719884052

21 Netina Tan, “Electoral Management of Digital Campaigns and Disinformation in East and Southeast Asia.” Election Law Journal: Rules, Politics, and Policy (2020), https://www.liebertpub.com/doi/pdf/10.1089/elj.2019.0599

22 Aim Sinpeng, “Digital media, political authoritarianism, and Internet controls in Southeast Asia” (2020)

23 Xinzhi Zhang and Wan-Ying Lin, “Stoking the Fires of Participation: Extending the Gamson Hypothesis on Social Media Use and Elite-challenging Political Engagement”, Computers in Human Behavior, Volume 79, 2018,

Pages 217-226, https://doi.org/10.1016/j.chb.2017.10.036.

Shin Haeng Lee, “Digital democracy in Asia: The impact of the Asian internet on political participation”, Journal of Information Technology & Politics, 14:1, (2017), pp. 62-82, DOI: 10.1080/19331681.2016.1214095

Min-hua Huang, Taehee Whang and Lei Xuchuan, “The Internet, Social Capital, and Civic Engagement in Asia”, Social Indicators Research volume 132, pp. 559–578 (2017), https://doi.org/10.1007/s11205-016-1319-0

[24] Ayesha Karamat and Ayesha Farooq, "Emerging Role of Social Media in Political Activism:

Perceptions and Practices", South Asian Studies: A Research Journal of South Asian Studies, Vol. 31, No. 1, January – June 2016, pp. 381 – 396,

http://pu.edu.pk/images/journal/csas/PDF/25%20Ayesha%20Karamat_v31_no1_jan-jun2016.pdf

Sanyarat Meesuwan, "The effect of Internet use on political participation: Could the Internet increase political participation in Thailand?", International Journal of Asia Pacific Studies 12 (2): 57–82, DOI: 10.21315/ijaps2016. 12.2.3.

[25] Natalie Pang and Debbie Goh, "Can blogs function as rhetorical publics in Asian democracies? An analysis using the case of Singapore", Telematics and Informatics, Volume 33, Issue 2, 2016, pp. 504-513, https://doi.org/10.1016/j.tele.2015.08.001.

[26] Michael Chan, Francis Lee and Hsuan-Ting Chen, "Examining the roles of social media use and connections to public actors on democratic engagement: An analysis of young adults in three Asian societies", New media & Society, pp. 1–18, 2021, https://doi.org/10.1177/1461444821105355

[27] Huang, Min-Hua, Ching-Hsuan Su, Ruixia Han et al, "How Does Rising Internet Usage Affect Political Participation in East Asia? Explaining Divergent Effects", Asian Perspective, vol. 41 no. 4 (2017): 527-558, doi:10.1353/apr.2017.0024.

[28] Xinzhi Zhang and Wan-Ying Lin, "Stoking the Fires of Participation: Extending the Gamson Hypothesis on Social Media Use and Elite-challenging Political Engagement", 2018.

Michael Chan, Hsuan-Ting Chen, and Francis L. F Lee, "Examining the roles of mobile and social media in political participation: A cross-national analysis of three Asian societies using a communication mediation approach", New Media & Society, 19(12), 2017. https://doi.org/10.1177/1461444816653190

Audrey Yue, Elmie Nekmat, and Annisa Betta, "Digital Literacy Through Digital Citizenship: Online Civic Participation and Public Opinion Evaluation of Youth Minorities in Southeast Asia", Media and Communication [Online], Volume 7 Number 2 (June 11, 2019), https://www.cogitatiopress.com/mediaandcommunication/article/view/1899/1899

[29] Margaret Andersen, "How Feminists in China are Using Emoji to Avoid Censorship", Wired, March 30, 2018, www.wired.com/story/china-feminism-emoji-censorhip

[30] "Guidelines for regulating digital platforms: a multistakeholder approach to safeguarding freedom of expression and access to information", UNESCO, CI-FEJ/FOEO/3Rev (2023) https://unesdoc.unesco.org/ark:/48223/pf0000384031.locale=en

DEPLOYMENT AND REGULATION OF TECHNOLOGY TO ENSURE RIGHTS

8. The Technological Infrastructure of Democracy.
Daniel Innerarity

Abstract

The relationship between technology and democracy is examined here from a fundamentally theoretical perspective in relation to the conceptual framework in which we should think about it. We cannot ask whether a technology is suitable for democracy if we do not address the kind of conditioning that technology exerts on humans, whether it is determinant, whether it is neutral, or whether it all depends on the use that is made of it. This chapter looks specifically at the case of algorithmic governance and asks about the desirability and feasibility of politicizing algorithmic decisions.

Technology, and especially digital technologies, have already become the main subject of expectations and fears about democracy. The future of democracy depends to a large extent on how we shape them and where they are placed within political procedures. An answer to the question of what democracy the current digital ecosystem enables or impedes requires prior reflection on the role that technology in general and technology in particular play in society.

Many of the current discussions on this topic are framed in binary terms: are new technologies good or bad? Does digitalization provide more freedom or does it restrict it? Should we expect algorithmic governance to enhance democracy or to eliminate it? Human life has unfolded in the tension between the utilities of technology and its threats. Optimists and pessimists posit scenarios that have in common that they grant technology too much power and reveal that they oversimplified the issue. Instead of technological determinism, what I propose is to explore the possible conditioning that digital technologies exert on democracy, which will allow us to examine to what extent algorithmic governance is capable of taking over political decisions and to answer the question of whether there will be an AI taking over democracy.

Technical conditioning is "the blind spot of democracy theory."[1] Digitalization should not be blamed for the current fragility of representative democracy; it can also be understood as a space of alternative possibilities. Exhaustion and distrust of representative institutions are also due to the shaping of a more active and demanding public opinion. To explain the current transformation of democracy solely in terms of digitalization is to overestimate the determinacy of technology and underestimate the capacity of political actors and institutions to take advantage of the possibilities that such technologies offer for democracy's revitalization. Digital media can be put at the service of both the liquidation and the revival of traditional (i.e., analog) politics. Digital technologies do not determine social and political change, but the can offer a potential (albeit limited) for distributed action. The relationship between digitalization and democracy should not be thought of as a causal relationship but as a constellation in which political action and modes of communication condition each other.

The relationship between technology and human decision-making

When Meta Platforms' CEO Mark Zuckerberg appeared before the US Senate to talk about misinformation, hate speech, and privacy, he proudly defended the technological solution: "artificial intelligence will fix everything in five to ten years." This "technosolutionism"[2] redefines complex social issues as problems that have computational solutions, i.e. it assumes that the power of technology is capable of solving any kind of problem. This conception of technology is also shared by certain governmental discourses and strategies that insist on the inevitability of technological development and the need to adapt to the economic opportunities it offers.

Technology solves many problems, causes some specific ones and, above all, raises the need to decide democratically what issues it is relevant for and to what extent. The advance of technology not only raises problems of applicability, but also of reconsideration of what we should understand as technologically solvable. The great democratic debate about technologies is about resituating them in a broad scope beyond the calculable world.

Although they may seem contradictory, technological neutralism and technological determinism are two ways of disengaging from the intertwining of the technological and the social. Neutralism and determinism conceive of technology independently of its social use, and as something closed, defined, and not susceptible to modulation; in the first case, because it is not necessary, and in the second, because it is not possible. Technology alters the landscape in which human interactions take place, but it does not facilitate every outcome. The cliché that "technology is just a tool" undervalues its capacity to structure situations, whereas its deterministic conception overvalues it.

Technological determinism often goes hand in hand with a reductionist view of technology that does not consider it as a social and cultural phenomenon such that technical devices are understood as predetermining their use without allowing each society to appropriate them according to its own idiosyncrasies and cultural patterns. If I draw attention to deterministic reductionism, I do not say this out of a lack of appreciation for technology, but quite the opposite: deterministic reductionism does not do justice to the whole phenomenon of technology, which consists not only of artefacts, but also of social uses and cultural dispositions within which technical innovations are put at the service of certain values.

Everything is affected by the technology we use, sometimes in very subtle ways, but this is not a question of seeing technology as a threatening reality; digitalization is not the problem, and thinking about it and carrying it out as something that does not require any format, any kind of express "political" intervention is. We must be careful not to neither consider political issues as technical issues nor consider technical issues apolitical.

My proposal is an alternative to neutralism and determinism that considers the relations between technology and society based on the idea of conditioning. Technology does not determine human actions or societies; it opens corridors that must be politically configured, and not everything is possible on the basis of the technology at our disposal. Instead of thinking of this conditioning as an unappealable determination, we would do better to understand it as an incitement to be critically examined, which allows choices to be made, albeit within a given framework. Each technology prevents certain things and compels, prompts, and discourages others. In between, there are plenty of indeterminate and open-ended choices.

The classic example of weapons well illustrates the limitations of the neutralist model. Some claim that a gun is neutral and it all depends on how it is used, whether to hunt or to kill.[3] This is a very simple statement. The question of conditioning does not refer to the possible use but to what the mere mass possession of weapons in a society, as is the case in the U.S., reveals. Their pervasive presence means not only mean that they could be used to kill, but also conceptions of individual sovereignty, conflict resolution, security, and justice are very different from societies where, as a rule, there are no guns in the home. Another example of this conditioning can be found in the series "Dopesick" about the wave of drug addiction that has recently spread in the U.S. as a result of the voracity of a pharmaceutical company and the ease with which opioid painkillers are prescribed. The owners of the pharmaceutical company, downplaying the risks of addiction, argue in their defense that they cannot prevent the misuse of painkillers, as if the problem lies solely with the consumers.

Something similar can be said of any technology and specifically of digital ones; they are more than media and assert a certain way of understanding and experiencing communication, space, time, work and opinion that is different from analog technologies. The misuse of social networks to offend and launch hoaxes is not an inevitability, but the ease of issuing opinions and the way in which collective trust is built or destroyed are some of the conditioning factors produced by the new digital space with which we are going to have to coexist. Neither will the network bear an irresistible democratization, nor will it necessarily degrade public discussion. We should not trivialize technology's conditioning force by appealing to its good or bad use. Democracy in the digital world will have properties about which we are still largely unaware.

Algorithmic governance and democracy

Governing is already to a large extent (and will become even more so) an algorithmic act; a large part of government decisions are taken by automated systems.[4] [5] One might call this system, in which algorithms are used to collect, collate, and organize the data on the basis of which decisions are made, an "algocracy."[6] Algorithmic governance greatly enhances management capabilities across large amounts of data and in relation to complex problems.

The spread of algorithm- and data-driven decision systems means that machines support humans in their decisions and even replace them, in part or completely. The question all this raises is to what extent and in what way the use of automated decision-making systems is compatible with what we consider a political decision-making system. What does the massive introduction of automated decision-making procedures for government action really mean? Is this type of governance congruent with democracy?

The great promise of this technology is that it allows us to know the real will of the people.[7] [8] With a world full of sensors, algorithms, data, and intelligent objects, a kind of social sensorium is configured that allows us to personalize health, transport, and energy. Thanks to data engineering, we are moving toward an increasingly granular understanding of individual interactions and systems that are better able to respond to individual needs.

Algorithmic systems serve to categorize individuals and predict their preferences from a wealth of data about them. The business model of many digital companies relies on the fact that they know users better than they know themselves and, by virtue of predicting their behaviour, can offer them the right thing at the right time. The comfortable paternalism of an algorithmic society is that it gives people what they want, that it governs with proportionate incentives, and that it anticipates, invites and suggests. Transposing this model to politics would not be a major problem were it not for the fact that the cost of these benefits is usually the sacrifice of some sphere of personal freedom. Given that there is a discrepancy in the self-determination we supposedly demand and the self-determination we are in fact willing to exercise when comforts and benefits are involved, the satisfaction of needs is often done in exchange for spaces of freedom.

What then is the democratic value of data, recommendations, and predictions? Some would say that all these are our free decisions from the past, invitations to decide in the present, or bets on how we will decide in the future, i.e., they are our decisions in any case. From this point of view, is no tension between Big Data and democracy. But democracy is not the immediate and aggregate translation of what we decide individually; the dynamic and transformative character of democratic life includes an element of change, discovery, and emergence for which a system designed to make us discover only what we already know is useless. At the present time, AI does not seem to be appropriate for this willingness to transform that is an essential element of our democratic decision-making.

The problem is that most algorithmic forecasts are based on the premise that the future will be as close as possible to the past, i.e., that our future preferences will represent a continuity of our previous behavior as recorded in our mobility or consumption data. Policy, however, does not aim only to reflect what is there. It changes certain things in an intentional way. Perhaps the most unsatisfactory thing about this data revolution is that it is not revolutionary at all. Data analysis acts as a recording device, to the point of having great difficulty identifying what there is in that reality of aspiration, desire or contradiction. But if we are to take our freedom seriously, it is also part of our aspiration to modify what we have been, thus giving rise to situations that are to some extent unpredictable. In this respect, algorithms that claim to be predictive are very conservative. They are predictive because they continually hypothesize that our future will be a reproduction of our past. They do not enter into the complex subjectivity of people and societies, where desires and aspirations also arise. How do we want to understand the reality of our societies if we do not introduce into our analyses, in addition to consumer behavior, the enormous asymmetries in terms of power, the injustices of this world, and our aspirations to change it?

Algorithmic governance is not a threat to democracy because it conditions our present decisions but, above all, because it disregards our future decisions. Democracy is not about doing what we want but, often, about being able to change what we want. Do algorithms really know our deepest will or only its most superficial dimension, the routines rather than the desires?

Politics is not simply a continuist administration of the past but the ever-open possibility of breaking the inertia of the past. How do we specify our goals such that machines have to do nothing but pursue them efficiently? Are we sure that what we want now will be what we want in the future? Machine learning algorithms can anticipate our future propensities and thus threaten to make alternative futures possible.[9]

A parliament of algorithms

Democratization is synonymous with politicization. If anything characterizes the political system of a democracy, it is that it is open to questioning, stimulates controversy, increases the number of interlocutors, does not prohibit new issues, does not exclude criticism as a matter of principle, and admits the configuration of alternatives. Politics is a reflexive thematization of life in common. Durkheim defined democracy as the political form of reflection.[10] The very vitality of a democracy shifts issues that were originally considered non-political into the space of the political. Many areas that were managed by the state and the protagonists of science and technology have been opened up to democratic discourse. Politics is about alternatives, options, interpretations, and perspectives. All positions, certainties, objectives, and decisions are provisional in principle and can be subject to revision.

All the technologies that accompany digitalization imply a greater depoliticization than previous technologies for at least two reasons: because of their exorbitant promises of de-ideologized objectivity and by virtue of their tacit and discreet nature. Let us examine the first of these promises. Algorithmic politics is a peculiar form of depoliticization in the name of objectivity. Algorithms depoliticize not because they are themselves apolitical but because they make it difficult or even impossible to deal politically with their results. The success of algorithmic techniques is not due to their ability to handle huge amounts of data but to their logic of incontestable clarity, their unambiguity, especially where there is little time or resources to decide. Algorithms are political when their results are beyond political questioning, i.e., when they depoliticize discourses, actions, and decisions.

The second peculiarity of algorithmic depoliticization is due to its thoughtlessness. The most radical conditioning and the most political dimension of digitalization takes place in a tacit space as a subtle modification of our individual and collective behavior. When we speak of the political dimension of algorithms, we must think not only of their use, but also of the specific logic with which they are inscribed in the social world. Digitalization not only makes life more efficient, faster, and more comfortable, but also modifies it in such a profound way that it is not easy to understand to what extent.

The democratic problem posed by both properties (de-ideologisation and unreflexivity) is not that algorithms make decisions but that we do not know or consent to them in some way. The question is whether we can in our turn politicize algorithms and consider algorithmic decisions as possibilities for our own self-determination or whether we have no choice but to surrender to them.

The compatibility of democracy and AI depends on their politicization, i.e., their insertion into broader contexts in which algorithms do with algorithms what modern democratic revolutions did with power: divide and problematize it, give it a limited term and limit its powers, expose it to contestation and criticism. If we do not accept that one authority can wield undisputed political power, then when algorithmic procedures are introduced into government, we must establish the spaces and channels that allow it to be questioned, monitored and audited. The increasing technification of political affairs must be balanced by a corresponding politicization of technical procedures.

It is in the nature of democracy to value technical and scientific evidence, as long as it does not call into question the pluralism of interpretations of reality or the diversity of ways in which such evidence can be brought into play when it comes to decisions in which other criteria also have to be asserted. In recent years, it has been emphasized that expert knowledge is more plural and that there are more epistemic authorities than are often assumed.[11] This principle of plurality should also apply when it comes to granting a monopoly of objectivity and validity to such epistemic procedures as algorithms and Big Data. The democratization of these technologies requires, as has always been the case when an authority of any kind has been configured, their insertion in spaces where the pluralism inherent to democratic societies is articulated.

We will mention a number of issues in which our digital environment precisely poses problems of lack of diversity and which would require ensuring pluralism. There is a lack of diversity in machine learning systems.[12] Lack of diversity in the very design of AI systems can reinforce discrimination by giving them an appearance of objectivity.[13] There is a whole discussion about how to achieve greater diversity in computer science, a discipline overly dependent on engineering and with a stereotypical model of masculinity.[14] We also have a problem in the balance of values when building and curating datasets,[15] The lack of facial diversity has led to identified discrimination in facial recognition that do not sufficiently take into account local and global differences.[16] [17]

If we cannot consider a society that limits pluralism as democratic, we should also be concerned with a lack of diversity in training data. There are not only parliaments where our political representatives sit; there must also be parliaments for them to discuss data, algorithms, and artifacts. This is what we are ultimately referring to when we talk about politicizing digitalization. Democracy in the digital age is impossible without an explicit thematization of technologies. Algorithms always involve choices between competing values that cannot be made on purely technical grounds and require extensive public deliberation. The "fairness" of algorithms must be understood as a political question and resolved politically, i.e., not optimising or improving algorithmic techniques but "considering and accommodating diverse, conflicting interests in a society."[18] This parliamentarisation of diversity can be found at the heart of the recommendation to companies and governments that when basing their decisions on machine learning they should "explore and enable alternative ways of datafying and modelling the same event, person or action" and the European Commission's proposal that automated processes should be explained in such a way that they can be "duly contested."[19]

Politicization always involves recognizing the constructive nature of political differences. We ought not renounce the epistemological advantages of institutionalized disagreement not only between humans, but also between us and our artifacts. We could even think of the metaphor of a parliament of algorithms and artifacts because there is not one technology but a variety of technologies that assert different procedures and principles. It is in this digital parliament that we would have to weigh and balance technological justifications, the validity of data, the biases of algorithms, the usefulness of automation in a way that resembles how we handle our ideological and interest differences in parliamentary institutions.

Conclusion

The debates surrounding the current development of technology are polarized around two positions: those who see this development as an external force that follows its own logic and to which everything must adapt (including states) and those who consider that there can only be legitimacy where a political centrality that accompanies and controls this technological development is assured. This polarization is at the origin of another dualism in our way of conceiving the new digital sphere: the utopia that posits that technology solves everything and the dystopia that sees only dangers. Both have a profoundly ahistorical vision that places power solely in technology and not in the way we humans appropriate it. This chapter argues for the necessity and resilience of politics as a human activity that is not replaceable by technology, although it should undoubtedly benefit from it. For all the shortcomings and dissatisfactions with the way politics is currently conducted, we do not seem to have found a functional substitute for that task which ultimately refers to a collective decision about the common issues that concern us. The great challenge ahead is to resist the charms of the depoliticization of our societies, overcome the inertia of traditional modes of governance, and not be seduced by the falsely apolitical discourse without insisting on practices that do not correspond at all to the new social realities. There is politics where, despite all the sophistication of calculations, we are finally compelled to make a decision that is neither preceded by overwhelming reasons nor driven by infallible technologies.

Endnotes

[1] Berg, Sebastian / Staemmler, Daniel (2020), “Zur Konstitution der digitalen Gesellschaft. Alternative Infraestrukturen als Element demokratischer Digitalisierung”, en Oswald / Borucki (ed.), *Demokratietheorie im Zeitalter der Frühdigitalisierung,* Wiesbaden: Springer, 127-147.

[2] Morozov, Evgeny (2013), *To Save Everything, Click Here: The Folly of Technological Solutionism,* New York: PublicAffairs.

[3] Pitt, Joseph (2014), "'Guns don't Kill, People Kill'", en Kroes, Peter / Verbeek (eds.) (2014), *The Moral Status of Technical Artefacts,* Dordrecht: Springer, 89-102.

[4] Pasquale, Frank (2015), *The Black Box Society: The Secret Algorithms that Control Money and Information,* Cambridge, MA: Harvard University Press.

[5] Lash, Scott. (2007), “Power after hegemony”, Theory, Culture & Society 24 (3), 55-78.

[6] Danaher, John / Hogan, Michael J. / Noone, Chris / Kennedy, Ronan / Behan, Anthony / De Paor, Aisling / Felzmann, Heike / Haklay, Muki / Khoo, Su-Ming / Morison, John / Murphy, Maria Helen / O’Brolchain, Niall / Schafer, Burkhard / Shankar, Kalpana (2017), “Algorithmic governance: Developing a research agenda through the power of collective intelligence”, *Big Data & Society,* July–December 2017, 1–21.

[7] Weizenbaum, Joseph (1976), *Computer Power and Human Reason: From Judgment To Computation,* San Francisco: W. H. Freeman.

[8] Martini, Mario / Nink, David (2017), “Wenn Maschinen entscheiden”, Neue Zeitschrift für Verwaltungsrecht 10, 1-14.

[9] Zuboff, Shoshana (2018), *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power,* New York: Public Affairs.

[10] Durkheim, Émile (2015) [1896], *Leçons de sociologie,* Paris, PUF.

[11] Jasanoff, Sheila (2007), *Designs on Nature. Science and Democracy in Europe and the United States.* Princeton, Princeton University Press.

[12] Fazelpour, Sina / De-Arteaga, Maria (2022), "Diversity in sociotechnical machine learning systems", Big Data & Society, January–June, 1–14.

[13] Mijatović, Dunja (2018), "In the era of artificial intelligence: Safeguarding human rights", Open Democracy blog, 3 July. https:// www.opendemocracy.net/ digitaliberties/ dunja-mijatovi/ in -era -of -artificial -intelligence -safeguarding -human -rights

[14] Zeising, Anja / Draude, Claude/ Schelhowe, Heidi / Maas, Susanne (eds.) (2014), *Vielfalt der Informatik: Ein Beitrag zu Selbstverständnis und Aussenwirkung,* Bremen.

[15] Scheuerman, Morgan Klaus / Denton, Emily / Hanna, Alex (2021), "Do Datasets Have Politics? Disciplinary Values in Computer Vision Dataset Development", Proc. ACM Hum.-Comput. Interact. 5, CSCW2, Article 317 (October 2021), https://doi.org/10.1145/3476058

[16] Hildebrandt, Mireille (2019), "Privacy as Protection of the Incomputable Self: From Agnostic to Agonistic Machine Learning", Theoretical Inquiries in Law, 20(1), 83-121.

[17] Eichler, Jessica / Topidi, Kyriaki (2022), *Minority Recognition and the Diversity Deficit Comparative Perspectives,* London: Hart.

[18] Wong, Pak-Hang (2020), "Democratizing Algorithmic Fairness", Philosophy & Technology 23, 225-244.

[19] High Level Expert Group on Artificial Intelligence, “Ethics Guidelines for Trustworthy AI” (2019), https://www.aepd.es/sites/default/files/2019-12/ai-ethics-guidelines.pdf

[20] Hughes, Thomas (1994), “Technological Momentum”, in Smith, Merrit Roe / Marx, Leo (eds.), *Does Technology Drive History? The Dilemma of Technological Determinism,* Cambridge, Mass: MIT Press, 101-113.

9. The role of an informed public in democratic systems.
D.J. Flynn

Abstract

Democracy requires citizens who are able and willing to update their preferences in response to relevant information. In recent years, changes in the information environment brought on by new technologies have raised concerns about the quality of political information available to citizens. This chapter reviews recent research into three such changes --- media fragmentation, social media, and fake news --- and potentially negative consequences. While these developments certainly pose new challenges for democracy, the research reviewed here shows that conventional wisdom overstates and misunderstands their potential consequences. For instance, "echo chambers" are not ubiquitous; social media often expose users to cross-cutting views; and fake news consumption is modest and concentrated among ideologically extreme citizens. The consequences of recent changes in the information environment, then, are more nuanced. Research shows that these changes may fuel polarization among already extreme citizens, reduce belief in true claims, and diminish feelings of trust and efficacy. After reviewing this research, the chapter concludes with a discussion of policy responses by governments, social media platforms, and other actors.

The functioning of democratic systems depends in large part on an informed citizenry. Even the most minimalistic conceptions of democracy acknowledge that citizens require certain types of knowledge to fulfill their democratic duties. For instance, retrospective models of democracy require citizens to monitor changes in objective conditions (e.g., unemployment, crime), accurately attribute credit or blame, and change their voting behavior accordingly.1 Other notions of democracy are more demanding. Deliberative democracy, for example, requires citizens to grasp substantial amounts of policy information in order to facilitate detailed exchange with their peers over policy alternatives.2 Despite these normative expectations, decades of survey data paint a dim picture of citizens' knowledge of public affairs.3 In recent years, a series of changes in the information environment brought on by new technology have raised new concerns about the quality of information available to citizens. Fortunately, a growing literature examines these technological developments and their implications for political knowledge, public opinion, and other normatively important outcomes (e.g., support for democratic institutions).

This chapter provides a critical review of this literature with particular attention paid to issues of democratic functioning. I begin by exploring the demographic, political, and informational predictors of individuals' factual beliefs using recently collected survey data from the United States. The remainder of the chapter then focuses on three recent changes in the information environment and their potentially deleterious effects: (1) media fragmentation and selective exposure, (2) social media and polarization, and (3) fake news and opinion distortion. In each of these areas, research suggests that the consequences of these technological developments are more nuanced — and less dire — than conventional wisdom suggests. I conclude with a discussion of recent attempts by governments and the private sector to deter potential negative effects of these new technologies.

The predictors of factual (mis)perceptions

Before discussing recent changes in the information environment, it is worthwhile to begin by examining the factors we know to be associated with citizens' political knowledge. To do so, I turn to recently collected survey data from the United States. Specifically, I rely on data from the 2020 ANES Time Series Study, which surveyed a representative sample of registered voters about their factual beliefs (among other topics) in the weeks before and after the 2020 general election.4 The surveys included several questions measuring factual beliefs, which I divide into two categories: knowledge of important features of the political system (Knowledge) and belief in a series of false or unsupported claims about politics and science (Misperceptions).5 Table 1 provides an overview of the issues considered in both categories.

Our goal here is to identify the factors that are consistently associated with holding accurate perceptions across a range of political facts. The ANES surveys include several questions measuring demographic characteristics, information sources, and political predispositions. This latter category includes measures of partisanship, left/right ideology, political interest, conspiratorial thinking, and populism. I estimated a series of statistical models predicting belief accuracy based on these variables.6 For ease of interpretation, I recoded all factual belief outcomes such that higher values indicate greater belief accuracy. Because of the format in which questions were asked, the Knowledge outcomes range from 0–1, and the Misperception outcomes range from 1–10 (see Appendix A for more information). In all models, positive (negative) coefficients indicate that the corresponding variable predicts more (less) accurate beliefs.

I consider the Knowledge and Misperception outcomes separately, starting with the Knowledge results in Table 2. As shown in the top panel of Table 2, demographics are consistent predictors of belief accuracy, with older, male, and college educated respondents holding more accurate beliefs about all four facts considered here. The gender finding is consistent with prior work and a large literature which explores possible reasons for the gender gap in political knowledge.7 Moving to the middle panel of Table 2, we see strikingly different results for traditional versus social media use. In particular, reading newspapers more regularly is positively associated with belief accuracy (3 of 4 facts), while more frequent social media use is negatively associated with belief accuracy (also 3 of 4 facts). Individuals who are frequent users of social media are consistently less accurate in their beliefs about the political system than individuals who rely on newspapers for their information, all else constant.

The bottom panel of Table 2 examines the role of political predispositions. Partisanship and ide- ology are not consistently related to belief accuracy. This is perhaps surprising in light of evidence that voters with partisan attachments and coherent ideologies are generally more knowledgeable than independents and non-ideologues, respectively. I further explore the role of partisanship and ideology below when considering the other outcomes.

By contrast, other predispositions are consistently related to accuracy. Political interest is positively associated with accuracy about all four facts considered here. Conspiracism, on the other hand, is negatively related to accuracy about all four facts. This consistent result is somewhat unexpected since the outcomes here are knowledge of structural features of the political system, which are not often subject to conspiratorial narratives. It appears that highly conspiratorial individuals are not only predisposed to endorse false or unsupported conspiratorial claims, but also less knowledgeable about the structure of political institutions and policy. Finally, populism is not a consistent predictor of accuracy, significantly predicting accuracy about only 1 out of 4 facts.

I now turn to the Misperception results, which are presented in Table 3. Starting in the top panel, we again see that demographics are consistent predictors of belief accuracy. Older, male, and college educated respondents consistently hold more accurate beliefs than younger, female, and non-college educated respondents, respectively. Turning to the information source results (middle panel), we see a familiar pattern: reading newspapers more regularly is a consistent predictor of holding accurate perceptions, while using social media more regularly predicts lesser accuracy.

Finally, looking at the bottom panel of Table 3, we see that several predispositions are again consistent predictors of belief accuracy. In contrast to the results discussed earlier, here we see that partisanship and ideology are consistently associated with belief accuracy. Interestingly, in most models, the coefficients on Democrat and Republican are significant but oppositely signed, which suggests that members of the two parties hold divergent factual beliefs (with Democrats holding more accurate perceptions of certain facts and Republicans more accurate perceptions of others). Comparing the results from the models more carefully, we can discern a clear pattern of selective learning: both Democrats and Republicans hold more (less) accurate perceptions of facts that are congenial (dissonant) to their preferred party.8 For instance, Democrats hold more accurate beliefs about Russian interference in the 2016 election, rising global temperatures, the origins of Covid– 19, and the safety and efficacy of hydroxycloroquine. In each of these cases, the factually correct answer is consistent with the factual claims of elite Democrats (e.g., Biden) or the party's preferred position (e.g., addressing climate change). By contrast, Democrats hold less accurate beliefs about deportations under the Obama versus Trump administration — the one claim on which the correct answer is uncomfortable for Democrats to acknowledge (i.e., that more illegal immigrants were deported in the first two years of the Obama compared to Trump administration).

The same pattern of selective learning is apparent among Republicans, though the results are less consistent and open to alternative explanations. Consistent with selective learning, Republicans hold less accurate beliefs about dissonant facts: Russian interference in 2016, rising global temperatures, and hydroxycloroquine. The mechanism is perhaps less definitive when we look to other facts where Republican congeniality is less clear. Republicans hold more accurate perceptions about two facts: deportations under Obama versus Trump and the consequences of vaccines. The deportations question is potentially congenial to Republicans because it refutes the conventional wisdom that Trump deported unprecedented numbers of immigrants early in his term.[9] Partisan congeniality is even less straightforward in the case of the vaccines/autism item, since vaccine skepticism is prominent on both the political left and right, though for different reasons.[10]

The two remaining predispositions — conspiracism and populism — are also consistent predictors of belief accuracy. Unsurprisingly, individuals with high level of conspiracism hold less accurate beliefs about virtually all facts considered here (5 of 6). More surprising, populism is associated with higher belief accuracy in 5 of 6 models — including those claims where (false) conspiratorial narratives are more prominent: global temperature patterns and the origins of Covid–

These positive associations between populism and belief accuracy hold under an alternative approach where the outcome is binary (i.e., correct answer or not).

To briefly summarize the empirical results, I find that:

- Demographics are consistent predictors of belief accuracy. Older, male, and college educated individuals hold more accurate beliefs than younger, female, and non-college educated individuals, respectively.
- Media sources are a consistent predictor of belief accuracy. More frequent use of newspapers predicts greater accuracy, while social media use predicts less accuracy.
- Two political predispositions — political interest and conspiracism — are consistent predictors of belief accuracy about the structure of the U.S. political system. Politically interested individuals are more accurate, while conspiratorial individuals are less accurate.
- A broader set of political predispositions — including partisanship, ideology, conspiracism, and populism — are consistent predictors of belief accuracy when it comes to misinformation. Partisans demonstrate selective learning, which results in more (less) accurate beliefs about partisan-congenial (partisan-dissonant) facts. Conspiracism is negatively associated with belief accuracy. Surprisingly, populism is positively associated with belief accuracy, though this finding is worthy of further exploration.

Of course, it is important to acknowledge that the relationships observed here may differ in other countries or on different factual issues. The U.S. political system is unique in several respects, notably its two-party presidential system and historic levels of polarization. However, recent re- search using data from other advanced democracies has reached conclusions largely in line with those offered here. For instance, one recent study into the predictors of fake news belief in Spain and Portugal reaches similar conclusions, with one notable exception: the study finds that populism is consistently associated with lower — not higher — belief accuracy.[12] Another study relying on data from nine European democracies finds that supporters of right-wing populist parties are consistently less accurate in their factual perceptions.[13] Collectively, then, evidence suggests that the relationship between populism and belief accuracy is likely contingent on the political context and specific facts considered.

Technology and the (mis)informed public

Since the invention of the printing press in the 15th century, technological innovations have regularly changed the volume and quality of political information available to citizens. In the early and mid-20th century, radio and broadcast television brought a limited number of high quality political news programs to wide swaths of the population. In the late 20th century, the advent of cable news resulted in an unprecedented number of political (and non-political) programs, giving consumers for the first time a significant degree of choice over the content they choose to consume. In the 20th century, the internet transformed the political information environment into a sea of almost limitless choice. In the opinion of many scholars and commentators, this high-information, high-choice environment has contributed to a series of problems that undermine democratic functioning. In this section, I provide an overview of research in this area. I focus in particular on three commonly discussed challenges in the contemporary information environment: (1) media fragmentation and selective exposure, (2) social media and polarization, and (3) the reach and influence of fake news.[14]

Media fragmentation and selective exposure

Media fragmentation refers to an increase in the number of available media sources (e.g., newspapers, television or radio shows, websites, etc.). As discussed, the introduction of cable news and the internet resulted in historic levels of media fragmentation. A common concern is that frag- mentation enables *ideological selective exposure*, which occurs when people self-select into media content that reinforces their existing preferences.[15] According to this line of thinking, which is often called the "echo chambers" or "filter bubbles" hypothesis, citizens navigate the information environment with an eye towards reinforcing their existing beliefs. This sort of self-selection may fuel extremism and hostility towards those with opposing views.[16]

While there are good reasons to expect that selective exposure may be widespread, especially during periods of polarization, there are also reasons to be more skeptical. Before considering the extent of ideological selective exposure, it is important to keep in mind that citizens first self- select into or out of political programming. Many citizens are uninterested in politics, preferring to spend their free time consuming entertainment rather than reading or watching political news.[17] Indeed, research has found that heightened media choice allows politically uninterested citizens to opt out of political news almost entirely. The introduction of cable television, for instance, allowed politically uninterested citizens to avoid political news and instead spend more time consuming entertainment programs. At the same time, the politically interested consumed more political news (and become more knowledgeable), exacerbating pre-existing knowledge gaps across politically interested and uninterested citizens.[18]

More recent research has reached similar conclusions about selective exposure into partisan cable programs[19] and online news.[20] One study that directly observed the internet search behavior of a representative sample of Americans found that people spend the vast majority of their time consuming entertainment (i.e., non-political) content.[21] Focusing on political news consumption, most people have relatively balanced media diets, consuming information from both left- and right-leaning sources.[22] Importantly, however, results indicated that the most ideologically extreme respondents do engage in substantial ideological selective exposure. While this group represents a small share of the general population, they are highly engaged in politics, which could give them outsize visibility and influence in the political process.

Social media and polarization

The proliferation of social media has heightened concerns about selective exposure. Of particular concern is the possibility that social media polarizes citizens by exposing them disproportionately to pro-attitudinal content.[23] The empirical evidence, however, again casts doubt on this possibility. Like the studies of online news consumption discussed above, research into social media finds that many users prefer non-political content. One recent study finds that approximately one-third of U.S. Twitter users do not follow any political accounts.[24] The same study found that users who do engage with political content on social media do so from a relatively ideologically balanced set of accounts.

Selective exposure is more prevalent among ideologically extreme social media users; however, even among this group there is a substantial amount of cross-ideological exposure. It is worth underscoring the important differences between users who frequently seek out political content on social media and those who do not. For example, a recent study found that Americans who report frequently commenting on Facebook hold more polarized opinions and write more toxic (i.e., vitriolic) comments compared to a national sample of Americans.[25] Moreover, this study found that toxic comments generate more Facebook likes and promote subsequent commenters to express more toxicity.

It would appear, then, that ideological selective exposure is less common than often assumed on both online news sites and social media platforms. The question then becomes why does polarization persist if most users are exposed to an ideologically balanced set of stories? One possibility— contrary to the "echo chambers" hypothesis — is that exposure to competing views fuels polarization via a process of partisan sorting.[26] According to this account, exposure to opposing viewpoints activates partisan identities and encourages "sorting" — a process whereby people are strongly motivated to adopt and defend the positions of their preferred parties. More evidence is clearly needed before making definitive conclusions about the mechanism(s) driving polarization, especially in light of the evidence discussed here.

Fake news and opinion distortion

A final concern in the contemporary information environment is the reach and potential distorting effect of *fake news*, defined here as false or misleading content that is presented with the intention to deceive readers. Using sophisticated web tracking methods, scholars have recently begun measuring fake news consumption directly, with one early study concluding that prominent fake news stories about the 2016 U.S. presidential election were shared millions of time online and more widely read than some mainstream stories.[27] While fake news consumption may appear widespread in absolute terms, it is important to consider the number and type individuals who are likely driving this consumption.

Recent studies using direct measures have concluded that fake news consumption is rare and concentrated among certain subgroups, especially older (65+) users and people for whom the fake news is politically congenial.[28] Returning to the 2016 U.S. election, evidence suggests that visits to fake news websites were rare and concentrated among Republicans, who presumably were already highly likely to support Trump. Two separate research teams using a similar methodology concluded that visits to pro-Trump fake news websites had no discernible impact on political attitudes or vote choice.[29]

Even if fake news exposure does not change attitudes or behavior among people who consume it, the presence of fake news in the environment may have broader, perhaps more deleterious effects. Fake news may, for example, depress turnout among key constituencies, decrease trust in legitimate sources of information, crowd out substantive topics from the political agenda, or decrease citizens' sense of efficacy.[30] If this line of thinking is correct, then fake news poses a significant problem even if it does not change the minds of users who directly consume it.

Policy responses

Technological innovations continue to transform the information environment in which citizens learn political facts and make political decisions. The prior section reviewed recent research into three such transformations: media fragmentation, social media, and fake news. In all three cases, research offers a more nuanced — and arguably less dire — picture of democratic functioning than conventional wisdom suggests.

One theme emerges from research in each of these three areas. The theme concerns the role of ideology in the mass public. In each of the three research areas reviewed here, ideologically extreme citizens behave differently than their less extreme peers. Specifically, ideologically extreme citizens are more likely to engage in ideological selective exposure on both news sites and social media platforms, to make toxic comments on social media platforms, and to consume and share fake news content. Similarly, recall from the data analyzed in the first section of this chapter that ideology (and partisanship) are associated with a selective pattern of learning: ideological (and partisan) citizens have less accurate beliefs about facts that are inconsistent with their predispositions. Collectively, this evidence suggests that ideological polarization — prevalent in many advanced democracies today — is likely to continue to fuel various threats to democracy.[31] It follows that reducing polarization is desirable not only for instrumental reasons (e.g., to improve policymaking), but also because it is likely to cultivate a healthier information environment with better informed citizens.

I close with a discussion of recent attempts by governments and the private sector to respond to some of the challenges discussed here, particularly fake news. I focus on efforts by three actors: social media platforms, policymakers, and journalists and other educators.

Social media platforms have recently adopted new policies to remove fake news and other harmful content (e.g., hate speech) and to sanction responsible users. Facebook established a putatively independent Oversight Board to supervise its content moderation practices. Facebook, Twitter, and other platforms regularly experiment with various real-time responses to fake news ranging from warnings about factually dubious posts to expert fact checks presented alongside all posts on particular topics (e.g., WHO information alongside Covid–19 tweets). Interestingly, different platforms have demonstrated varying levels of willingness to tolerate potentially harmful content or engage in aggressive content moderation. For instance, Twitter reversed many of its content moderation policies following Elon Musk’s purchase of the company. According to some observers, these sorts of policy reversals and inconsistencies across platforms highlight the need for industry-wide regulations from governments or international organizations.

While the specific threats to democracy have evolved, the challenges governments face in regulating potentially dangerous speech have not. Governments vary considerably in the relative weight they place on free speech versus regulation of potentially dangerous speech (compare, e.g., the US and Germany). A fundamental issue for government concerns transparency and objectivity. Government attempts to intervene in the marketplace of ideas will be viewed skeptically by many citizens, especially those who distrust the incumbent government or perceive the particular intervention as politically motivated. Research into public opinion on free speech issues generally finds that citizens have malleable opinions on the issue and are open to restrictions on speech if they are justified with compelling arguments.[32]

Finally, journalists and educators have reformed many of their practices in response to the challenges discussed in this chapter. In journalism, recent years have witnessed the institutionalization of fact-checking, with independent fact checkers now operating in over 100 countries and connected via an International Fact-Checking Network. At the same time, a large academic literature investigates best practices in fact-checking, focusing on factors such as the source, timing, and se- mantic structure of corrections.[33] Educators are also investing considerable resources into boosting digital literacy and other upstream approaches focused on fake news discernment.

Technological innovation continually reshapes the political information environment. Resulting threats to democracy continue to evolve. Policymakers and the public will be well served by data-driven policy responses that take account of findings from studies like those reviewed here.

Endnotes

1 Fiorina, M. P. (1981). Retrospective Voting in American National Elections. Yale University Press.

2 Fishkin, J. S. (1991). Democracy and Deliberation: New Directions for Democratic Reform.

3 Delli Carpini, M. X., & Keeter, S. (1996). What Americans Know about Politics and Why It Matters. Yale University Press. / Converse, P. E. (1964). The Nature of Belief Systems in Mass Publics. In Ideology and Discontent (Apter, Ed.). University of Michigan Press. / Taber, C. S., & Lodge, M. (2006). Motivated Skepticism in the Evaluation of Political Beliefs. American Journal of Political Science, 50(3), 755–769.

4 American National Election Studies. (2021). NES 2020 Time Series Study Full Release [dataset and documentation]. www.electionstudies.org.

5 The knowledge items were asked in the pre-election phase of the survey; the misperception items were asked in the post-election phase.

6 The models are OLS regressions.

7 Dolan, K. (2011). Do Women and Men Know Different Things? Measuring Gender Differences in Political Knowledge. Journal of Politics, 73(1), 97–107.

8 Past research has uncovered a similar pattern of selective learning among both citizens (Jerit & Barabas, 2012) and elites (Lee et al., 2021).

9 On the other hand, if Republicans in the sample support increasing the number of deportations, then the fact that Trump deported fewer illegal immigrants than Obama is arguably dissonant.

10 Roberts, H. A., Clark, D. A., Kalina, C., Sherman, C., Brislin, S., Heitzeg, M. M., & Hicks, B. M. (2022). To vax or not to vax: Predictors of anti-vax attitudes and COVID-19 vaccine hesitancy prior to widespread vaccine availability. PLOS ONE, 17(02), 1-19.

12 Wiesehomeier, N., Busby, E., & Flynn, D. J. (Forthcoming). Populism and Misinformation. In The Ideational Approach to Populism: Consequences and Mitigation (Chryssogelos, A., Hawkins, K. A., Hawkins, E. T., Littvay, L., & Wiesehomeier, N., Eds.). Routledge.

13 van Kessel, S., Sajuria, J., & Van Hauwaert, S. M. (2021). Informed, uninformed or misinformed? A cross-national analysis of populist party supporters across European democracies. West European Politics, 44(3), 585-610.

14 Prior, M. (2007). Post-Broadcast Democracy. Cambridge University Press.

15 Other scholars refer to the same phenomenon as partisan selective exposure. The same logic holds.

16 Sunstein, C. R. (2007). Republic.com 2.0. Princeton University Press.

17 Delli Carpini, M. X., & Keeter, S. (1996). What Americans Know about Politics and Why It Matters. Yale University Press.

18 Prior, M. (2007). Post-Broadcast Democracy. Cambridge University Press.

19 Levendusky, M. S. (2013). How Partisan Media Polarize America. University of Chicago Press.

20 Guess, A. M. (2021). (Almost) Everything in Moderation: New Evidence on Americans' Online Media Diets. American Journal of Political Science, 65(4), 1007-1022.

21 Guess, A. M. (2021). (Almost) Everything in Moderation: New Evidence on Americans' Online Media Diets. American Journal of Political Science, 65(4), 1007-1022.

22 Cardenal, A. S., Aguilar-Paredes, C., Cristancho, C., & Majo-Vazquez, S. (2019). Echo-chambers in online news consumption: Evidence from survey and navigation data in Spain. European Journal of Communication, 34(4), 360-376.

23 Sunstein, C. (2017). #Republic: Divided Democracy in the Age of Social Media. Princeton University Press.

24 Eady, G., Nagler, J., Guess, A., Zilinsky, J., & Tucker, J. A. (2019). How Many People Live in Political Bubbles on Social Media? Evidence From Linked Survey and Twitter Data. SAGE Open, 9(1), 2158244019832705.

25 Kim, J. W., Guess, A., Nyhan, B., & Reifler, J. (2021). The Distorting Prism of Social Media: How Self-Selection and Exposure to Incivility Fuel Online Comment Toxicity. Journal of Communication, 71(09), 922-946.

26 Törnberg, P. (2022). How digital media drive affective polarization through partisan sorting. Proceedings of the National Academy of Sciences, 119(42).

27 Allcott, H., & Gentzkow, M. (2017). Social media and fake news in the 2016 election. Journal of Economic Perspectives, 31(2).

28 Guess, A., Nyhan, B., & Reifler, J. (2020). Exposure to untrustworthy websites in the 2016 US election. Nature Human Behaviour, 4(5). / Guess, A., Nagler, J., & Tucker, J. (2019). Less than you think: Prevalence and predictors of fake news dissemination on Facebook. Science Advances, 5(1).

29 Eady, G., Paskhalis, T., Zilinsky, J., Bonneau, R., Nagler, J., & Tucker, J. A. (2023). Exposure to the Russian Internet Research Agency foreign influence campaign on Twitter in the 2016 US election and its relationship to attitudes and voting behavior. Nature Human Behaviour, 14(1). / Bail, C. A., Guay, B., Maloney, E., Combs, A., Hillygus, D. S., Merhout, F., Freelon, D., & Volfovsky, A. (2020). Assessing the Russian Internet Research Agency's impact on the political attitudes and behaviors of American Twitter users in late 2017. Proceedings of the National Academy of Sciences, 117(1), 243-250.

30 York, C., Ponder, J. D., Humphries, Z., Goodall, C., Beam, M., & Winters, C. (2020). Effects of Fact-Checking Political Misinformation on Perceptual Accuracy and Epistemic Political Efficacy. Journalism & Mass Communication Quarterly, 97(4), 958-980.

31 Svolik, M. W. (2019). Polarization versus democracy. Journal of Democracy, 30(3), 20–32.

32 Chong, D. (1993). How People Think, Reason, and Feel about Rights and Liberties. American Journal of Political Science, 37(3), 867–899.

33 Flynn, D.J., Nyhan, B., & Reifler, J. (2017). The Nature and Origins of Misperceptions: Understanding False and Unsupported Beliefs About Politics. Advances in Political Psychology, 38, 127–150.

Further references

New Haven, CT: Yale University Press.

Jerit, Jennifer, and Jason Barabas. 2012. "Partisan Perceptual Bias and the Information Environ- ment." *Journal of Politics* 74 (March): 672–684.

Lee, Nathan, Brendan Nyhan, Jason Reifler, and D.J. Flynn. 2021. "More Accurate, But No Less Polarized: Comparing the Factual Beliefs of Government Officials and the Public." *British Journal of Political Science* 51 (3): 1315–1322.

10. Right to Truth, Right to Privacy and Right to Know. Abuses and the way out.

Marcin Kilanowski

Abstract:

The international law refers to the right to truth. A similar right exists on the national level, which is the right to information. However, the right to information may get into conflict with the right to privacy. While legislators and courts tried to find a proper balance between the two and the scholars started to think about developing the right to truth on the level of national jurisdictions, the notions of truth, information and privacy became highly challenged with the intensive development of new technologies. The information and data obtained by tech companies, political parties and governments became means for development of disinformation and "fake news" in light of economic or political interests of these entities on the national or international ground. There is much disturbing evidence of the activities undertaken by the mentioned actors in various political campaigns dating from around 2010, including the use of hacking, of disinformation, and of voter suppression through alleged violence and intimidation. We should ask the question whether it is still possible to defend the idea of reaching for the truth, gaining information and knowledge while respecting the right to privacy and right to freedom in democratic societies. A positive answer shall include a set of recommendations.

Introduction

We are facing a crisis in our democracy – the crisis of the notion of truth and knowledge, as well as difficulties in getting access to information and with protection of privacy due to the systematic manipulation of data that supports the relentless targeting of citizens, without their consent, by campaigns of fake news, disinformation and messages of hate. The prevalence of the fake news phenomenon can be mainly ascribed to the popularity of social media as channels of communication between people. Drawing knowledge from a small number of sources and closing oneself in information bubbles favors the spread of false content. Some researchers emphasize that although projects aiming to counter disinformation are implemented both at the national and international level, the chance of controlling this phenomenon is small.[1] Social media, where the content is based on private opinions of users, will always be subjective. As Internet users have the right to express their own opinion, based on personal knowledge and experience, it is mostly up to the readers and viewers themselves to assess the credibility of the information they encounter. The awareness of citizens is the greatest potential weapon in the fight against fake news; thus we need to educate the society in critical thinking, as well as to disclose sources of information and enable the Internet users to have greater control over search results. Moreover, we need new legal and institutional arrangements.

In this article I will firstly focus on the clash between the right to information and the right to privacy, and how they are at risk due to the development of new technologies. In light of that risk, it is also a crucial question whether it is still possible to obtain unbiased knowledge about the world, whether the truth can be protected from falsification, and whether it is possible to speak about the "right to truth". The aim of this article is to answer two questions: How to search for the truth and to protect the truth today in the times of new technologies? What actions may help us deal with new technologies, considering the opportunities and threats they pose? In conclusion, the article will present a set of recommendations that can help overcome the difficulties and dangers that our societies and democratic systems started to face due to the development of new technologies. The recommendations can be a basis for legal regulations concerning education, freedom of speech, journalism, corporate governance, and state responsibility that will help to use the new technologies for the common good instead of the benefit of the few.

From international law to national law

On March 24, 1980 human rights defender Archbishop Óscar Arnulfo Romero was assassinated. On each anniversary of this event, the international community pays tribute to his legacy by celebrating the Day of the Right to the Truth Concerning Serious Violations of Human Rights and the Dignity of Victims. In the doctrine of public international law, the right to the truth about gross violations of human rights is an inalienable and autonomous subjective right. The right to the truth is linked with the right to justice and redress, and the guarantee that abuse will not happen again.

The United Nations and other international organizations support a number of activities aimed at disclosing the facts of serious violations of human rights and international humanitarian law. These activities are designed to promote justice and equity, encourage redress and recommend reforms of abusive institutions. The UN created the Commissions of Inquiry in the Central African Republic, Syria and the Democratic People's Republic of Korea, as well as established the Tunisia Truth and Dignity Commission and other similar initiatives. In 2012 Human Rights Council also appointed the Special Rapporteur to achieve the mentioned goals, who since then, has analyzed some of the challenges facing the truth committees in transition, presenting also proposals for actions to improve the effectiveness of these mechanisms. [2]

On a national level, legal acts do not refer so far to the right to truth, but to the right to information. The right to information is linked with the access to public information, i.e. with transparency. Many countries emphasize the importance of transparency for the effective functioning of democratic mechanisms, social control over the exercise of power and the protection of citizens’ health. Access to information on public affairs determines the ability to control whether the state really serves the interests of its citizens. Such information is valuable only if it is consistent with reality, i.e. verifiable and objective. Access to information should be exercised in light of the basic principles of a democratic state, which are openness, transparency and the pursuit of finding out the truth, as well as in light of some exceptions — allowed in a few cases and provided for by law – which are confidentiality, secrecy and the prohibition of disseminating knowledge on a specific topic.[3]

The right to information is also connected with the right to obtain information about persons discharging public functions. In a democratic state ruled by law, it is acknowledged that people need to know more about public officials than about other people. In consequence, public officials must take into account the fact that, due to the function they perform, their privacy is limited, and thus the resulting conflict between the right to public information and the protection of the right to privacy in relation to persons performing public functions is inevitable. In other words, in the case of persons performing public functions, the right to information clashes with the right to privacy, which include in particular (based on acts of national and international law together with the jurisprudence of international tribunals): the right to personal inviolability, the right to protect family life, the right to the inviolability of the home, the right to freedom and protection of confidentiality of communication, the right to information autonomy. This list is considered as one that should be reflected in every branch of law in which privacy should be understood as a sphere of life that every person wants to keep only for themselves.[4] It is understood that each person has a certain intimate sphere of feelings, thoughts and beliefs, which they want to keep secret only from others, even from the closest people. The undisturbed existence of this sphere guarantees proper human development and provides psychological comfort. Moreover, it is a sphere where an individual wants to be free from the interference of other people, where they can independently decide about their own life and make personal choices. Using it, a person has the opportunity to freely establish contacts with other people according to their own choice, the ability to decide on the scope of disclosure of information concerning themselves, and freely develop their life and fulfil their own personality.

The mentioned right to privacy is limited not only in the case of persons performing public functions but also of citizens when state interest is at stake. In such circumstances the right of the state – the public interest – clashes with the private right. This is the right to information about the activities of ordinary citizens in order to protect and ensure security, public order or morality, the rights and freedoms of other people, to prevent crimes and to punish perpetrators, while providing the public with information about the course and results of pending criminal proceedings. In this way, the state and the law in a democratic system protects against individuals, groups, and movements that from the point of view of the axiology of the system are of an extreme nature, by prohibiting certain behaviors as well as the dissemination of certain ideas that can threaten the existence of democracy, so that they do not threaten freedom and the search for truth. That is why several kinds of activities have been excluded from social life or limited. Limitations were also imposed on the concept of “free market of ideas”, and legal limitations were introduced to the right to freedom of speech.[5]

Right to truth?

A democratic state, whether social or liberal, differs from a totalitarian or authoritarian state, which limits an individual's autonomy not only by interfering with their privacy, but also by limiting the freedom of expression, movement or association, claiming the right to dissemination of the "truth" and the monopoly to impose what this truth is.[6] In a democratic state, the space for search of the truth is much wider also with regard to the truth about the state's actions. In a complex world, people should be able to search for the truth and to protect what they know, especially about the actions of the state. The basic, general principle on which a democratic state operates is and must be openness, transparency and access to the truth. Confidentiality or secrecy are admissible in truly exceptional situations, in which we are dealing with strategic areas related to state security, or the sphere of the already mentioned privacy. Openness and transparency allow the citizens to check whether the state really acts in their interest. Openness therefore should be the norm, not the exception, if state or local government officials are to act in the interest of society. This applies to recent and current actions but also to past ones. Thus it is understood that citizens have the right to know the historical truth about actions and events – also from the point of view of criminal, civil or political responsibility of those who made certain decisions. The established historical truth is often understood as the one that should be protected. To do that, certain views are excluded from the public discourse as "public untruths", while states introduce criminal sanctions example.g. for denying the historical facts. Over the past several decades, regulations have been adopted regarding various forms of the so-called historical lie through "the right to memory". [7] Most often, such legal regulations are related to the crimes of the 20th century and the functioning of totalitarian regimes. The law prohibits denying, minimizing, trivializing, justifying or condoning genocide as well as denying crimes against humanity. [8]

The problem of "public untruth" is a very current issue. It is especially challenging to protect the "truth" in light of the phenomenon of mass disinformation taking the form of fake news. In such circumstances it seems reasonable to claim that people should have the right to know because ""the desire for truth is deeply rooted in the nature of every human being, whose conduct, if he acts in accordance with that nature, is subordinated to the demands of truth". [9] However, such words show that even in a democratic state, one can be tempted to think that our actions are to be "subordinated to the demands of truth", ignoring the need to protect the sphere of freedom and privacy of citizens. Such thinking can quickly devolve towards authoritarianism.

Thinking about the truth as a category separate from freedom – especially freedom of speech – is very common nowadays. The term "truth" is used very often and in various circumstances. Citizens of many democratic countries including Poland, Hungary or the US are often faced with the "obvious truth", the acceptance of which is a condition of being classified as a wise person or a true patriot. Satisfying such "truth" is a pretext for constantly calling press conferences at which the "truth" is announced and loaded onto media vehicles in order to transport it towards the recipients. Too often, however, those who speak in the name of the truth believe that have the monopoly to satisfy it, but they do not prove the truthfulness of what is said. They want everyone to accept it, and anyone who is against is an enemy.[10] What counts is their version of truth and not that of others. mentioning noteworthy example are the events that led to the development of the social platform Truth Social by Donald Trump, advertised as the medium that was supposed to present the truth, unlike Twitter or Facebook. Not long after the development of the platform it has been widely accused of censorship. [11] According to an August 2022 report from consumer rights advocacy group Public Citizen, Truth Social was found to censor liberal and progressive users that disagreed with the site's narrative. In June 2022, several accounts were reportedly banned by Truth Social after posting about investigations into the 2021 United States Capitol attack and the January 6 hearings that detailed events leading up to the mob violence on that day, in which Trump supporters breached the United States Congress, seeking to overturn the 2020 presidential election. Public Citizen concluded that Truth Social's content moderation was more limiting than Twitter's, and that Truth Social's policies were "creating an echo chamber of violent views". [12]

Having truth as a reference point was supposed to help prevent the development of authoritarian tendencies; however, nowadays it is often used by those that commit atrocities in the name of the "truth" or "right to truth". They use the language that points out to "truth", but in fact they limit freedom of speech and they are involved in dissemination of untrue, inaccurate or misleading information, which today reaches much further and wider due to the use of new technologies.[13] Therefore, it should be ensured that in a democratic state the desire to know the truth does not undermine basic civil rights such as the right to privacy, the right to defend one's good name, and the right to freedom of expression. Desiring to know the truth, one should not forget that the superior good is another person.

New technologies: the right to information and right to privacy at risk

One of the needs of humans as individuals is the need to maintain privacy, yet nowadays privacy is one of the goods most at risk and thus among the most desired and valued. There is the risk of the state trying to know more than necessary about its citizens. This is mainly due to the emergence of modern image- and sound-recording devices. Another risk is posed by the rapid development of new technologies allowing access to private information about the citizens. Such risk is also posed by other actors, such as corporations or political parties, which may use so obtained information in a way that can threaten the security of citizens as well as of the state. The problem in this case is surveillance, but also what the acquired information can be used for. Among the threats are restricting citizens' access to truthful information or to information that presents different points of view, as well as dissemination of intentionally mileading information. Through such actions, the private lives of individuals are influenced and controlled, while the scope of individual freedom and access to knowledge is limited. Ubiquitous digital surveillance takes away people's privacy and dignity, often reducing them to recipients of commercials.

It is certain that to some extent the mentioned new technologies offer a better access to information and knowledge. The development of modern technologies and the digital environment enables easy acquisition of information, access to many sources of knowledge and its sharing on an unprecedented scale. At the same time, the digital revolution, which is taking place also through social media, has completely changed the ways of sharing information and communication between people, facilitating these activities but also creating additional opportunities for surveillance and shaping citizens' opinions, e.g. by spreading false information. When the recipients do not verify knowledge in other sources, they do not have a full picture of reality, and information garnered from social media is the only one available to them.

New technologies, including the Internet with its huge global network of interconnected computers that knows no national borders as well contains the largest database of all kind of information can negatively affect the lives of citizens. They may also threaten the security of these citizens as well as the information security of the state, which consists in striving to ensure the functioning and development of both the state and the society free of interference, through free access to information, while maintaining the ability to influence information.[14] Phenomena such as trolling, post-truth, fake news and deep fake are examples of particular key threats today. What all of these phenomena have in common is a desire for profit. Internet trolls are paid for their actions. Misleading content published on websites affects the growing interest in them and helps earn money from advertising. Catchy pieces of news are used to attract attention in order to gain publicity, which is associated with financial but also political gain. Another type of political profit from disinformation can involve destruction of the image of politicians or authorities. This raises the concern of scientists, because disinformation can pose a threat to the democratic political process, as well as to any decision-making process based on rational criteria. With the rapid evolution of technologies, the right to privacy, the right to information, the right to education and the search for truth are being abandoned. This may lead to an increase in radical and populist attitudes, which poses a threat to the existence of democracy.[15]

Truth: the way to protect it

It must be noticed that the right to information is linked with the right to education. In many countries information rights are guaranteed by the basic laws[15], and so is the right to education. The particular objective of access to information and education is to gain knowledge and learn the truth. This truth is considered a condition for scientific, cultural or social development, and as such is one of the highest values of Western civilization. The possibility of knowing it is inscribed in the classical concept of truth, which is based on the assumption that the known facts correspond to reality; however, our ability to understand and describe that reality has always been questioned, also by philosophers of science and sociologists of science.[16] In the Modern era, a question has been asked with increasing frequency: what are facts and what is reality?. Among the critics of the classical concept of truth was Michel Foucault, who claimed that the truth "is the most recent illusion", and so is our knowledge about it. According to Foucault, knowledge is shaped by social practices, and reaching the truth is questionable because the cognitive process and the acquisition of knowledge are entangled in a struggle for power. He claimed that ""power produces knowledge [...] that power and knowledge are directly related; that there are no power relations without a correlated field of knowledge, and no knowledge that does not presuppose and does not create power relations".[17] In other words, there is no knowledge independent from power relations. These relations shape what is presented to us as "the knowledge" and "the truth". In fact, this is not the objective knowledge and the truth but the one that serves the interests of some. Appropriate discourse and social practices are created to support the process of pursuing these interests.

Foucault was one of the pragmatists, critical theorists and postmodernists, who also criticized the classical conception of truth. They all questioned whether we can gain knowledge, at least the objective one. We also see very well how hard it is for the scientists to establish objective truth, for example regarding the healthiness of GMO food or causes of climate change or appropriate retirement age in particular countries.[18] These issues are tightly connected with conflicting economic and political interests. It is equally hard to gain true information and objective knowledge about past and present decision processes. This casts doubts as to whether such processes can be truly transparent, not only because sometimes they take place without full knowledge and understanding of persons involved, but also because those who think they knew the reasons for their decisions sometimes claim the necessary secrecy regarding state activities or evoke the business judgment rule.[19]

Following this line of reasoning, we see how knowledge is entangled in power, in political or economic decisions. However, Such thinking can be dangerous because it can lead to arguing that "everything is political". The claims of postmodernism can sustain all those practicing the dissemination of subjective opinions as equally valid and denying the possibility of talking about objective facts and thus about truth and knowledge. Reaching for the argument that television is "political", that legislators, prosecutors, judges or the academy is "political", makes us slowly slide towards authoritarianism as what matters is the subjective opinion of this or that "political" group – a power-holding group which wants to win for itself as much space as possible not by force of argument but by argument of force.[20] Why argue when there is no truth to discover?

When Foucault's considerations are no longer just a philosophical narrative and become the reality, we hear the voices that we must defend the truth in the face of a deluge of fake news. Some argue that it is possible, although it is not easy. They argue that defending the truth requires effort, diligence, courage and determination. It remains hidden and we must be careful not to miss it. Plato claimed that truth and knowledge are the fruit of effort, the result of a long philosophical search.[21] Relying on the belief that obtaining knowledge is possible is one thing though, and obtaining it is another. Who should be nominated as a guardian of the truth? Those that are designated to do it are scientists, even though they are often in disagreement with each other, as already said. Another way to gain knowledge and establish the truth is through the work of a group of experts; yet their work may be contested by other groups of experts – even more so when the issue is political or when interests of particular groups in the society are involved, which is most often the case.[22] Thus it is sometimes more appropriate to establish fact finding commissions or truth and reconciliation commissions, composed of representatives of different stakeholders, of different views, but always those that are interested in resolving the issue and finding the truth. In their work they rely on the willingness of all to engage in dialogue, in common effort to search for the answer.[23] Finding the truth may also happen through litigation. From Nuremberg to The Hague, the truth has been many times established through court proceedings – although there are allegations that the tribunals operating in these cities were established by victors. Undoubtedly, it is important that the courts adjudicate impartially and independently, which is the case only in democratic countries, when a court decision is the result of applying the law and not issuing judgments as required, as was the case with the courts that convicted Navalny or Poczobut.[24] Such rulings are highly controversial for some – and so are for others the rulings of the European Court of Justice and European Court of Human Rights pointing out that Poland and Hungary violated the rule of law. The governments of these countries claim that they are only defending Christian values and their sovereignty; Poland has not complied with the judgments, calling them political and untrue.[25] A future International Criminal Court ruling in The Hague on charges against Putin for war crimes in Ukraine will also be recognized only by some.[26]

Apart from the work of scientists, experts and court litigation, which is often based on the work of scientists and expert committees, we unfortunately have no other tools to determine what the truth is or what actions should be taken to achieve the right or true result, expected state or goal. It is also necessary to be aware that regardless of the contested result of the search for truth, it will be always based not on what the facts were or are, but on what claims about facts were considered confirmed, justified or proven. It will also have to be based on freedom of speech.

As in every debate – whether social, political or legal, whether conducted on newspaper front pages or in the chambers of parliaments, university premises, or in courts – a necessary precondition to search for the truth is the freedom of speech. We need such freedom to speak about how to search for the truth, what is the truth or how we should understand it. As John Stuart Mill said, freedom of speech is necessary; however, it should not be used to irresponsibly say whatever one wants to say, but to search for the truth.[27] He argued that a prevailing opinion or common knowledge on any matter can be wrong, and there is no chance of rectification if people do not have the right to express their views. And thess people often know best when they face difficulties, when the "shoe pinches" as John Dewey pointed out. [28] Even if they are might only be partly true, the freedom to question what we know or believe can lead to the discovery of aspects that were not known or recognized before; for example, that women should have voting rights. However, it is important to choose the right moment to do so, as Mill advises. What is important is not only that the truth is told, but also the way in which it is conveyed. The more difficult the truth, the more care should be taken to express it. Questioning the *status quo* or the common knowledge should happen when the emotions are low because that will enable people to listen to each other's arguments and will lead to better understanding of others. [29] According to Isaiah Berlin, another famous proponent of the necessity for freedom in our private and public life, freedom that we have should lead to better understanding. For that, Berlin added, we need tolerance, which requires showing respect to the others.[30] Jurgen Habermas adds to Mill's and Berlin's prescription for a healthy society a requirement to undertake the communication that is governed by communicative rationality, and not merely the rationality that is directed toward achieving a particular goal, because that aim can be far from the goal of discovering the truth.[31] Such communication should be based on equal treatment of those that speak or equal treatment of the parties involved in dialogue, which rests on the respect of the dignity of all. There should be mutual respect between speakers – Even if what they do or think is not be respected, they themselves should be respected.

Conclusion: not the right to truth but the right strategy

Knowing the truth is important, because by knowing it we can make adequate decisions. In the face of the information crisis, there are more and more voices pointing out to the need to protect such truth by means of law. [32] There are proposals of public law solutions to guarantee and secure the truth in various areas of public affairs. [33] Some refer to such right, but "the right to truth" refers to an idea and not to a positive law with a specific content. The involvement of the law as the guardian of the truth, however, raises doubts related to fears of introducing censorship, which can lead to violations of freedom of speech. This freedom is important in the process of discovering the truth, as it protects us from the danger of closing ourselves from gaining full knowledge in the best case, and in the worst, from creating conditions in which some people use "the one and only truth" as a justification for developing authoritarian rules.[34] Freedom of speech is therefore necessary for expressing claims, presenting arguments, gaining knowledge and uncovering the truth. Only in some cases it is easy to establish the truth – for example, what was the speed of the car that left skid marks on the street after the driver hit the brakes. Most of the time, searching for the truth will require a long process of discovery and will be a source of conflict. And even though we may not like the fact that there is conflict, some level of it will and should exist, as disagreement is natural when different views are confronted, and it is the basis for new discoveries. The inquiry process should, however, always rest on the willingness of those who disagree to search for the answer, with mutual respect among the opponents.

We operate in a world of complexity, which requires a lot of our attention. We are bombarded with data informing us about the world and with untrue statements about it. In the course of time, we have accumulated knowledge, yet unforeseen situations happen, which shows the limitations of our knowledge and ability to predict the cause of action, making us realize that we cannot be certain what may happen tomorrow. [35] To master this complexity, we adopt strategies or procedures. They may prove helpful in search for truth if we adjust them to changing conditions, in addition to the existing forms of seeking the truth through court proceedings and the work of expert groups or commissions. So far, when making an account of profits and losses ensuing from the expansion of new communication technologies, at the expense of our privacy and often identity, we gain access to an unlimited amount of information, which might be true but also manipulated. The goal should be to develop such strategies that will allow us to protect not only our privacy but also access to information and prevent the spread of disinformation on the Internet. On the basis of various reports, it is possible to present key recommendations as to strategies and procedures that should be adopted for this purpose [36]:

Education in critical thinking

The ability to critically assess the credibility of information, questioning attitude, willingness to search for an answer, not taking everything for granted on the basis of the information provided, as well as the culture of continuous learning – all this should form the basis of education in the field of new technlogies. Education systems should be adapted to the new reality;– instead of preparing pupils to assimilate truths, teach them critical thinking. The fight against fake news, information bubbles, and intentional manipulations should start with education and sensitizing young people to the fact that what appears on the web is often intentionally or unintentionally spread falsehood. The ability to recognize fake content is a key skill in using information in the modern world and can be the basis for counteracting the phenomenon of fake news.

Empowerment of journalists and users

It is important to sensitize media employees to the issue of using verified source material as well as support independent news media and promote high-quality journalism. What is more, users themselves should have more knowledge and control over the results they receive from search engines. It is important to filter information not only for its accuracy, but also for the quality of the source. Readers and viewers should also be able to report cases of fake news.

Transparency

Users should be able to distinguish journalistic content from other information, including private posts and opinions. They should also be able to verify the sources, for example, to ensure that political advertising on social media platforms includes clear information on its source, including the author, the country of origin and the sponsor(s). To ensure better transparency, online platforms also should conduct their own analysis of fake news and inform users when false content has been published. If it is discovered that they are involved in practices of spreading disinformation, they should be banned from the possibility of earning from advertising.

Clear responsibility and liability of tech companies

Tech companies are not passive platforms – they reward what is most engaging according to their business model and growth strategy. They profit by using such model and therefore they should be held responsible and liable for harmful and misleading content shared on their sites. That should include conventional criminal sanctions for individuals and financial penalties for digital platforms that do not remove false information in time.

Non-financial auditing of tech companies

Companies are required to conduct financial audits. The same type of auditing should be required for non-financial activities of technology companies. They should report about their security mechanisms and algorithms in order to ensure that they operate responsibly. This should also concern the use of fake accounts on social media and advertising that targets people with disinformation, for example during election periods. It would require developing a specialized state control service which, as in case of tax control or labor inspectors, would control algorithms used by large technology companies to process and transmit information, for example in social media.

Digital Charter

It is important that the digital rights of users are guaranteed in every country. Establishing a Digital Charter as a new legal mechanism would present legal obligations, terms of liability and user protection in signatory countries.

Endnotes:

[1] See: Olan, F., Jayawickrama, U., Arakpogun, E.O. et al. Fake news on Social Media: the Impact on Society. Inf Syst Front (2022). https://doi.org/10.1007/s10796-022-10242-z

[2] Pablo de Greiff, Report of the Special Rapporteur on the promotion of truth, justice, reparation and guarantees of non-recurrence, Report of the Special Procedure of the Human Rights Council, information, A/HRC/30/1 3, Geneva : UN, 7 Sept. 2015

[3] More on that see: Hollyer, James, Peter Rosendorff, and James Vreeland. 2011. "Democracy and Transparency." Journal of Politics 73 (4): 1191-205.

[4] Rubenfeld, Jed. “The Right of Privacy.” *Harvard Law Review* 102, no. 4 (1989): 737–807.

[5] Gunatilleke, G. Justifying Limitations on the Freedom of Expression. *Hum Rights Rev* 22, 91–108 (2021).

[6] Fetter, Frank Albert. “Planning For Totalitarian Monopoly.” *Journal of Political Economy*, vol. 45, no. 1, 1937, pp. 95–110.

[7] Koposov, Nikolay. Memory Laws, Memory Wars: The Politics of the Past in Europe and Russia. Cambridge University Press, 2017.

[8] For example sixteen European countries, as well as Canada and Israel have laws against Holocaust denial. More on that see: Whine, Michael. “EXPANDING

HOLOCAUST DENIAL AND LEGISLATION AGAINST IT.” *Jewish Political Studies Review*, vol. 20, no. 1/2, 2008, pp. 57–77.

[9] https://bip.brpo.gov.pl/pliki/1162808841.pdf

[10] Max Brändle, When everyone is your enemy, IPS, 07.06.2023, Available: https://www.ips-journal.eu/topics/democracy-and-society/when-everyone-is-your-enemy-6758/.

[11] "Truth Social's Inexplicable Censorship, Heavy-Handed Terms of Service Defy Free Speech Promises". Public Citizen. August2, 2022. Available: https://www.citizen.org/news/truth-socials-inexplicable-censorship-heavy-handed-terms-of-service-defy-free-speech-promises/

[12] See: Leonard, Kimberly. "Trump's purported free speech social media platform Truth Social is hiding user posts, threatening to create a 'curated echo chamber,' research group finds". Business Insider. August 3, 2022. Available: https://www.businessinsider.nl/trumps-purported-free-speech-social-media-platform-truth-social-is-hiding-user-posts-threatening-to-create-a-curated-echo-chamber-research-group-finds/; :”Truth Can’t Handle the Truth. Censorship on Truth Social”, Public Citizen. August 2, 2022.

[13] Jack Grieve, Helena Woodfield, The Language of Fake News, Cambridge University Press, Cambridge 2023.

[14] Chyba, Christopher F. “New Technologies & Strategic Stability.” *Daedalus*, vol. 149, no. 2, 2020, pp. 150–70.

[15] Watts, Clint. “Disinformation’s Dangerous Appeal: How the Tactic Continues to Shape Great Power Politics.” *The Fletcher Forum of World Affairs*, vol. 44, no. 2, 2020, pp. 19–28.

[16] See: Art. 61 of the Constitution of the Republic of Poland, art. 31 of the Constitution of Romania, art. 100 Constitution of Norweg.

[17] More on that see: Gerald Vision, Veritas: The Correspondence Theory and Its Critics, The MIT Press, Cambridge 2004.

[18] Foucault, Michel, Discipline & Punish: The Birth of the Prison. Translated by Alan Sheridan, Viking, London 1977, p. 27.

[19] On that see: Carolan, Michael S.,“ The Multidimensionality of Environmental Problems: The GMO Controversy and the Limits of Scientific Materialism.” *Environmental Values*, vol. 17, no. 1, 2008, pp. 67–82.

[20] More on the role of business judgment rule see: Marcin Kilanowski, Deep Capture: The Hidden Role of Rationalizations, Psychology and Corporate Law, And What Philosophy Can Do About It, in: Philosophy in the Time of Economic Crisis, Pragmatism and Economy, Stikker K. W., Skowroński K. P. (eds.), Routledge, New York 2018, pp. 108-125.

21 Sadurski Wojciech, Poland's Constitutional Breakdown, Oxford University Press, Oxford 2019.

22 Kaufman, Daniel A. “Knowledge, Wisdom, and the Philosopher.” *Philosophy*, vol. 81, no. 315, 2006, pp. 129–51.

23 See: Kennedy, David, A World of Struggle: How Power, Law, and Expertise Shape Global Political Economy, Princeton University Press, New Heaven 2016.

24 More on that: Hirsch, Michal Ben-Josef, et al. “Measuring the Impacts of Truth and ReconCiliation Commissions: Placing the Global ‘success ’of TRCs in Local Perspective.” *Cooperation and Conflict*, vol. 47, no. 3, 2012, pp. 386–403.

25 Litvinova, Dasha, Russian court sends an associate of Kremlin foe Navalny to prison for 7 1/2 years, AP NEWS, June 14, 2023; Karmanau Yuras, Belarus upholds 8-year prison sentence for journalist of top Polish newspaper, AP NEWS, May 26, 2023.

26 Erlanger, Steven, Pronczuk Monika, Poland Escalates Fight With Europe Over the Rule of Law, The New York Times, July 15, 2021, https://www.nytimes.com/2021/07/15/world/europe/poland-hungary-europe.html

27 "Situation in Ukraine: ICC judges issue arrest warrants against Vladimir Vladimirovich Putin and Maria Alekseyevna Lvova-Belova". International Criminal Court. 17 March 2023, https://www.icc-cpi.int/news/situation-ukraine-icc-judges-issue-arrest-warrants-against-vladimir-vladimirovich-putin-and

28 Ryan, John K. “Truth and Freedom.” *The Journal of Higher Education*, vol. 20, no. 7, 1949, pp. 349–52.

29 John Dewey, “Democracy and Educational Administration,” in *The Later Works of John Dewey*, vol. 11, ed. Jo Ann Boydston (Carbondale: Southern Illinois University Press, 1987), 217–26, at 218.

30 John Stuart Mill, On Freedom, p.

31 Isaiah Berlin, Two Concepts of Freedom, p.

32 Jurgen Habermas, The Theory of Communicative Action, p.

33 Karol Dobrzeniecki, „Prawo do prawdy” w perspektywie filozoficznoprawnej. Przyczynek do dyskusji, Z Zagadnień Prawoznawstwa, Wrocław 2020, pp. 73-85.

34 Kurt Wagner, Facebook Is Building An Oversight Board. Can That Fix Its Problems? The new, independent group will review controversial choices made by content moderators, Bloomber, 24 June, 2019. https://www.bloomberg.com/news/articles/2019-06-24/facebook-is-building-an-oversight-board-can-that-fix-its-problems.

35 Of course there is nothing wrong in believing that there is truth or having a believe that one knows the truth. The issue is how one uses that knowledge. See: Marcin

Kilanowski, Abandoning truth is not a solution. A discussion with Richard Rorty, in: Diametros 61/2019, pp. 34-50.

36 Some call it black swans. Payzan-LeNestour, Elise. “Can People Learn about ‘Black Swans’? Experimental Evidence.” *The Review of Financial Studies*, vol. 31, no. 12, 2018, pp. 4815–62.

37 For example: Digital, Culture, Media and Sport Committee “Disinformation and ‘fake news’: Interim Report”, House of Commons, HC 1791, February 2019; Digital, Culture, Media and Sport Committee, "Disinformation and 'fake news': Final Report”, House of Commons, HC 1791, February 2019; ENISA, Strengthening Network and Information Security to protect the EU against fake news”, April 27, 2018

11.Improving political representation through data.
Peter Loewen

Abstract

A central assumption of democratic government is that representatives know important things about the citizens they represent. Successful governments wish to know what their citizens want them to do now and in the future. Politicians, political staffers, and political advisors seek to know the needs and political preferences of their voters and constituents. In some cases, politicians will seek to know the behaviour of citizens, and how it is related to government policy. Central to this assumption related democratic representation is another assumption: politicians have available the information required to learn about citizens.

In this chapter, I do three things. First, I provide context for some of the on-the-ground facts which outline the gap between what we want our politicians to know and what they can know. I then briefly review the kinds of data that could improve representation. I next discuss two broad areas of political representation and public policy making that could be materially improved by a greater engagement of data by politicians and public servants. I conclude by considering how various democratic values and practices not only make it possible for public servants and politicians to engage in more systematic learning, but also confer an advantage to democracies.

It is important to acknowledge upfront that taking learning from data seriously may not be an existential crisis for democracies, but, regardless, it is a major one. At no time since the end of history[1], ie. the end of the cold war, has there been such a contest of systems as there is today. Conflict in Ukraine underscores a fragile European political system. Populism and antisystem sentiment represent a breaking down of the trust required to make democratic delegation work. In contrast to these faltering systems, and no matter how bumpy recent times have been, China's ascent is even more remarkable. Underwriting much of China's governance success is an unyielding commitment to knowing what its citizens are doing, what they are thinking, what they care about, and how well they are being served by their local and regional governments [2]. Systems of constant surveillance and social crediting fundamentally and negatively change the relationship between citizens and their state. But if one side of the coin is a total surveillance state, the other side is a belief that governments should know as much about what citizens want and think as possible so that that government can do its job better. Arguably, the problem with China is not the ambition of knowing everything about its citizens, but rather wishing to use this information to assert control over citizens rather than democratically respond to free citizens. In this, China is not alone among authoritarian states, just ahead of its contemporaries in how much progress the state has made and control China has been able to assert over its citizens.

What if democratic states committed themselves to knowing just as much in the aggregate about their citizens, while using this information democratically, in a manner that was respectful both of privacy and the democratic liberties of citizens?

What do politicians know about citizens? What do they know about policy?

A classic, if simplified, way of thinking about the roles of politicians in a democracy is to classify them as delegates or trustees [3]. Delegates believe that their central function is to deliver in government the policies that citizens want. Trustees, by contrast, are not so interested in doing what citizens want as they are in delivering on what citizens need, even if citizens cannot easily articulate (or know) those needs. In this framework, good delegates will know what citizens want them to do (ie. their preferences) and good trustees will not know about the facts of their voters' lives or what their constituents need from government.

On the knowledge side, a growing body of evidence suggests that politicians in democratic countries are often systematically biased or incorrect in their perceptions of what citizens want. This has been well-documented in the United States, where a clear conservative bias exists in politicians' perceptions of citizens' preferences[4 5]. But it exists elsewhere, too. For example, [6] show that politicians have similar conservative biases in five other countries, and [7] show that politicians in several countries are not even all that good at identifying on what side of an issue a majority of citizens fall. On balance, the evidence suggests that politicians do not know what citizens want across a variety of issues. Other studies suggest that they might not be all that interested in even learning about citizen preferences [8], perhaps because it is so difficult to access timely and relevant data. This is contrary to much earlier evidence which suggests strong linkages between constituency preferences and politicians' actions [9]. Whether politicians are in fact getting worse at knowing citizens' preferences is beside the point, largely. The bottom line is that they do not know what citizens want as well as we might expect or as much as democratic theory suggests.

Politicians are not only grasping to determine what citizens want. They also have a difficult time understanding what citizens need. Rather than being guided by systematic data, politicians are often animated by narratives that focus on how a single individual or a small group of people are helped by a policy. Such empathic personalizing actually impairs good judgment about group needs [10]. When politicians are tested on their knowledge of the material well-being of their constituents, the most recent evidence suggests that they have systematic errors in their perceptions [11]. Politicians, for example, do not accurately estimate the financial hardships of their constituents. How can they then be expected to effectively work on citizens' behalf if they do not systematically understand the needs and stations of their citizens?

Finally, politicians (and other public servants) might be expected to care about the effects of the policies which they propose and then implement. But there are limits to this, too. Politicians are often reluctant to pursue information extensively when designing policies [12], and they often show little interest in understanding how well policies are actually affecting citizens on the ground.

Can we rethink how politicians learn about citizens?

Perhaps it is unreasonable to expect politicians to know everything which a citizen wants them to do. This is especially true given how expensive data has often been. For a long time, learning about citizens' preferences and behaviours was both costly and difficult [13]. Learning was costly because studies of citizens' preferences often required high quality public opinion studies, which took a long time to collect and were also prohibitively expensive. Learning about their behaviours similarly required active and costly data collection. Moreover, knowing the material status and needs of individual voters with some frequency - ie. not relying on a decennial census - was out of reach. What is more, learning was often constrained because for ethical or legal reasons, it was not possible to (easily) collect data about citizens.

In many ways, technology changes this relationship. Politicians can get information on citizens' preferences much more easily. The collection of public opinion data has become remarkably more economical in recent years through various online data methods. Other methods, like sentiment and text analysis, allows researchers to learn about latent and expressed preferences passively or unobtrusively.

Through advances in “big data” and the processing of high dimensional data, we can also learn more quickly what services citizens are accessing, and how these uses are related to each other. For example, by merging administrative data sources, analysts can learn how access to one government service – for example, income supports – may relate to demand for another service – for example, health care provision. And, through mobility data especially, politicians can learn a lot about patterns of government service usage. In short, the ability to engage data about citizens in policymaking is greater than ever.

How could politics improve with more data engagement?

In this section, I provide two sketches of how politicians and public servants could better engage existing high frequency or high dimension data sources to learn more about what citizens want, and what they need and how policies are positively or negatively addressing those needs.

Knowing what citizens want

Knowing what citizens want should be a straightforward enough enterprise. Politicians can simply poll constituents, querying their views on key issues, and then learn from the results of those polls. There are at least four limits to traditional polling techniques, however. First, public opinion studies suffer from substantial problems of non-response bias, where some types of citizens (perhaps a majority) are unwilling to answer surveys, thus limiting the representativeness of survey results. Second, polls are often limited in space, constraining how many issues can be queried or the depth at which they can be sounded. Third, because they can be expensive, polls occur with limited frequency. Finally, polls are typically conducted on samples which, while sufficient to make national level inferences, are nonetheless too small in any single sample to learn about important subgroups, whether demographic or geographic. Consider, for example, a group which represents 5% of the population. In a representative sample of 1000 citizens, just 50 citizens from this group will be present, substantially limiting how much can be learned about that group compared to others.

What can be done in the face of such constraints? There are at least three solutions on offer, which in combination can substantially enhance how much politicians know about citizens preferences. First, more sources than simple polls can be used to measure citizens’ preferences. Recognizing that public preferences are often latent - that they lie below the surface but that they are revealed through what people say, how they respond to polls, what they like, forward, and retweet online, even what they buy - we can model how supportive citizens are of some courses of government action over others by correlating large amounts of data across multiple sources. Second, we can use modern statistical techniques of imputing outcomes - in this case preferences - to precise demographic groups or geographies, through techniques like multiple regression post stratification. Combining together multiple data sources and then modeling them down to the kinds of small micro-targeted groups politicians care about, can help politicians know what different groups in different geographies want. And by relying on more than just poll data, this can be updated with high regularity.

Imagine, then, a dashboard which for any issue in front of or potentially in front of a legislature would provide a legislator with detailed data about the preferences of citizens, which could be queried at not only a general population level, but for subsets of the population the politician is interested in. Direct, rich, and frequently updated data could empower politicians to represent citizens’ preferences much better than they currently do.

Knowing what citizens need

The commercial world is awash in information on consumers. Individuals generate data across thousands of transactions, internet searches, movements, and other behaviours. Importantly, while these are often individual actions, it is possible for these data to be stitched together. Accordingly, we learn not only about what is happening in the aggregate, but what identified individuals are doing. For any given person, we can potentially understand their movement history, the state of their individual finances, detailed demographic information, information on their personal professional relationships, and even information on their preferences for dating. Many rightly regard this kind of information as intrusive and in violation of basic norms of privacy, an entirely reasonable position. And yet commercial organizations go to great effort to assemble these kind of data within legislated privacy regimes precisely because there is immense value in accurately understanding important information about the lives of consumers.

Do politicians know as much about the people they represent? Do they know how often their constituents are able to access healthy food options within their neighborhoods? Do they know how much individual constituents have to travel for work, commute to receive Medical services, or venture out for recreation? Do they know how often their constituents are expressing concern or experiencing stress over their financial state, through for example search data, accessing their own credit reports, or even asking their financial institutions for short-term help? And, most importantly, can they understand how a policy change would affect any of those things?

The long story short is that in many countries, politicians have a much fuzzier view of the lives of their citizens than the average marketing agency or Swift security corporation, and even less of a sense of how a policy would change individuals' lives. At one end of this extreme is the Canadian case, where federal and provincial bureaucracies do not collect systematic digital health data, where there is almost no easy linkage of data at an individual level across multiple departments, and where the national statistics agency cannot easily access information - even in a highly controlled manner - on individual financial holdings. By contrast, Nordic democracies and Israel collect massive amounts of health and social data on citizens, and incorporate this into policy decision making at a granular level. In place of systematic data on the effects of policies and the lives of their constituents, politicians instead lean on impressionistic accounts from interactions with constituents or from received correspondence, or they turn to information provided by interested lobby groups or policy advisors.

Imagine instead a scenario in which politicians were able to understand at the level of individual constituents, whether their financial situations were improving or deteriorating week over week, whether they were experiencing more or fewer health challenges, or in more general terms, whether they needed more or less intervention from the state to help their lives flourish, and in what areas of their lives. Suppose that politicians could have access to high frequency, high detail data-driven accounts of how well their constituents are faring materially, and what kinds of government assistance could be effectively targeted to them. Imagine too that the tools of causal inference were applied to these data, to understand how the deployment and uptake of support policies actually did or did not improve the lives of citizens. Such policy making would require a substantial bargain between government and citizens: that citizens would be willing to give over large amounts of their data, and that government could be trusted to use these data in a manner consistent with democratic ends and not in a manner that violates privacy or other democratic norms.

The Democratic Advantage

In the battle for data, surveillance, and learning, it is sometimes argued that autocratic regimes have a natural advantage. They are unconstrained by high citizen expectations of privacy and are often not bound by effective legal regimes which enforce those protections and other rights. Moreover, unconstrained by democratic processes, they can move with great rapidity to change course when they learn about new states of the world. In comparison, democratic government is said to be overly concerned with privacy and handcuffed by partisan fighting and by checks and balances.

This discourse, however, fails to see at least three reasons why democratic governments could benefit from the use of high dimensional data and applied artificial intelligence to learn about and act on citizens preferences in a way that autocratic regimes cannot.

The first reason is the "values premium" that exists within democracies. Embedded within democracies is the notion that how citizens are treated matters as much as what citizens get. Process matters as much as outcomes. Democracies put a premium on values like trust, transparency, and decency. In the evocative example of Avishai Margalit in his work, The Decent Society, we are asked to consider the difference between delivering bread in a famine from the back of truck, where in one scenario it is handed to recipients and in another it is thrown at their feet to be scrambled after. In both scenarios the same outcome results: people get food. But only in one are citizens treated decently. That makes all the difference. Democracies are practiced - especially at the level of "street level bureaucrats" - at treating people with decency, as rights-bearing individuals. This premium on values and process and not just on outcomes, is one part of the democratic advantage.

Second, democracies are naturally better at incorporating feedback. This "feedback advantage" comes from the competitive nature of democracies. Autocracies suffer from inefficient feedback mechanisms, as public criticism of state action is regularly short-circuited. Instead of soliciting genuine, organic measures of satisfaction among citizens, autocratic states impose order and assume all is well among citizens. By contrast, the competitive incentive in democracies to find out what governments have done well and poorly invites constant refinement of processes and policies. The same would apply in cases in which governing officials are using large amounts of data to learn about and act on the preferences of citizens.

Finally, there is a public sector advantage. Compared to private organizations, democratic public services are arguably more culturally ready for the adoption of this technology than any other organization, precisely because public services already resemble human-assisted AI systems. A public servant is already used to working within a prediction machine: they are presented with a problem, they formulate and test solutions using data, and they then make recommendations through a series of considerations—or algorithms—which is eventually placed before a human to make a choice from a small number of options. That final decision maker is the human in the loop, and while they cannot see all the deliberations and considerations that lead to a recommendation, they have a responsibility to own the decision and to be able to explain and justify it if demanded. All these elements map onto a well-designed system of human-assisted AI.

Conclusion

Politics is a difficult job, done by humans. Those humans are limited in their capacity to imagine the preferences of others and to understand their needs. Effective democratic governance depends on us enhancing the capacity of public figures to know and effectively act upon citizens' wants and needs. The availability of data and our capacity to learn from it is increasing at a breathtaking clip. By taking seriously the insights afforded through the combination of data, artificial intelligence, and machine learning, public servants can better know what it is citizens want them to do and what citizens need them to do, and by leaning in directly on the values already embedded in democratic systems, the need for decency, the need for aligning values with actions, and the need for democratic accountability and explanation, makes our public systems ironically as ready as any to unlock the gains provided by this combination of data and learning tools.

Endnotes

1 Fukuyama, F. (1989). The end of history? The National Interest, 16, 3-18.

2 Leonard, M. (2008). What does China think? PublicAffairs.

3 Fox, J., & Shotts, K. W. (2009). Delegates or trustees? A theory of political accountability. The Journal of Politics, 71(4), 1225-1237.

4 Hertel-Fernandez, A., Mildenberger, M., & Stokes, L. C. (2019). Legislative staff and representation in Congress. American Political Science Review, 113(1), 1-18.

5 Broockman, D. E., & Skovron, C. (2018). Bias in perceptions of public opinion among political elites. American Political Science Review, 112(3), 542-563.

6 Pilet, J.-B., Helfer, L., Sheffer, L., Varone, F., Vliegenthart, R., & Walgrave, S. (Forthcoming). The Conservative Bias Among Politicians: A Five Country Comparative Study. American Political Science Review.

7 Walgrave, S., Jansen, A., Sevenans, J., Soontjens, K., Pilet, J.-B., Brack, N., Varone, F., et al. (2023). Inaccurate Politicians: Elected Representatives' Estimations of Public Opinion in Four Countries. The Journal of Politics, 85(1), 209-222.

8 Kalla, J. L., & Porter, E. (2021). Correcting bias in perceptions of public opinion among American elected officials: results from two field experiments. British Journal of Political Science, 51(4), 1792-1800.

9 Miller, W. E., & Stokes, D. E. (1963). Constituency influence in Congress. American Political Science Review, 57(1), 45-56.

10 Bloom, P. (2017). Against empathy: The case for rational compassion. Random House.

11 Thal, A. (2023). Do Political Elites Have Accurate Perceptions of Social Conditions? British Journal of Political Science. (Forthcoming).

12 Loewen, P. J., Rubenson, D., & McAndrews, J. R. (2022). When Do Politicians Pursue More Policy Information? Journal of Experimental Political Science, 9(2), 216-224.

13 Fenno, R. F. (1977). US House members in their constituencies: An exploration. American Political Science Review, 71(3), 883-917.

Further references

Druckman, J. N., & Jacobs, L. R. (2006). Lumpers and splitters: The public opinion information that politicians collect and use. Journal of Public Opinion Quarterly, 70(4), 453-476.

Gilens, M., & Page, B. I. (2014). Testing theories of American politics: Elites, interest groups, and average citizens. Perspectives on politics, 12(3), 564-581.

Henderson, G., Hertel-Fernandez, A., Mildenberger, M., & Stokes, L. C. (2021). Conducting the heavenly chorus: Constituent contact and provoked petitioning in congress. Perspectives on Politics, 1-18.

CONCLUDING ESSAY

12. The Need for a New Social Contract.
Elisabeth Braw

Abstract

'The problem is to find a form of association which will defend and protect with the whole common force the person and goods of each associate, and in which each, while uniting himself with all, may still obey himself alone, and remain as free as before,' Jean-Jacques Rousseau observed in *The Social Contract.*[1] The Swiss philosopher stood in a long line of thinkers who, beginning with Socrates, had set out how societies could combine citizens' individual freedom (including freedom of speech) with society-wide rules of engagement preventing a descent into anarchy as citizens exercised their freedom. The arrival of mobile phones, the internet and social media has, over the past three and half decades, established an entirely new way for citizens to interact with one another and society as a whole, and this digital revolution will further accelerate as artificial intelligence and the internet of things take on a larger role in daily life. This chapter lays out the need for a new social contract suited to the digital age, and how to create it.

'The problem is to find a form of association which will defend and protect with the whole common force the person and goods of each associate, and in which each, while uniting himself with all, may still obey himself alone, and remain as free as before.' This is the fundamental problem of which the Social Contract provides the solution,' Jean-Jacques Rousseau observes in *The Social Contract.*[2] In the treatise, published in 1762, the Swiss philosopher outlined how societies should be organised in a way that allowed citizens the freedom to exercise their free will without this leading to anarchy. Since the arrival of the mass-produced mobile phone and easily accessible internet around the same time, and social media around a decade later, citizens have been able to pursue virtually limitless technology-aided pursuits, often in isolation from fellow citizens. While offering vast benefits of knowledge and convenience, modern technologies have thus eroded the social contact among citizens and as a result the unwritten social contract that governs liberal democracies.

Long before 1762 humans had organised themselves, whether merely at the family level or all the way up to the nation-state level in ways of greater or lesser harmony. Many centuries earlier, Socrates had argued that societies needed social contracts in order to function well, and closer to Rousseau's time John Locke and Thomas Hobbes had made similar arguments. Indeed, for almost as long as Socrates's thoughts have existed, thinkers inside and outside seats of higher learning have occupied themselves with social-contract theory, 'the view that persons' moral and/or political obligations are dependent upon a contract or agreement among them to form the society in which they live'.[3] As Rousseau noted, 'Men can't create new forces; they can only bring together ones that already exist, and steer them. So their only way to preserve themselves is to unite a number of forces so that they are jointly powerful enough to deal with the obstacles. They have to bring these forces into play in such a way that they act together in a single thrust. For forces to add up in this way, many people have to work together.'[4] In some cases, including cantons in Rousseau's native Switzerland and German cities' self-governing burgher councils, the citizens involved had considerable agency. But by and large, despite the efforts by Socrates, Locke, and Hobbes to establish codes that would combine citizen freedom and agency with a functioning society that almost everyone could endorse, pre-enlightenment citizens had little say because their societies' rulers mostly them as societal participants without the need for agency. Most did, in other words, not have access to social contracts in any setting above the most local ones. Conversely, this meant that rulers' power was based solely on their exercising of that power, not on popular consent.

The Enlightenment set out to change that. 'Find a form of association that will bring the whole common force to bear on defending and protecting each associate's person and goods, doing this in such a way that each of them, while uniting himself with all, still obeys only himself and remains as free as before,' Rousseau advised.[5] The movement in which he was such a key participant helped trigger reforms for more citizen rights and participation in countries across Europe.

With this definition of the social contract, Rousseau places himself firmly in the thinking established by Socrates. Indeed, by definition the social contract is a set of rules of behaviour that all parts of society agree on. Such an effort must start with Rousseau's instruction to 'find a form of association that will bring the whole common force to bear on defending and protecting each associate's person and goods' and continue with John F. Kennedy's inaugural address. 'In the long history of the world, only a few generations have been granted the role of defending freedom in its hour of maximum danger. […] The energy, the faith, the devotion which we bring to this endeavour will light our country and all who serve it — and the glow from that fire can truly light the world. And so, my fellow Americans: ask not what your country can do for you — ask what you can do for your country,' the US President declared at his inauguration in 1961.[6]

Ask what you can do for your country: this is a central part of any social contract. It is also an area in which liberal democracies' existing social contracts have dangerously deteriorated. A hundred years ago it was clear to a critical mass of citizens of liberal democracies what constituted their role in their societies: in addition to paying taxes and obeying laws, looking after elderly relatives, treating fellow citizens with respect. That was important because one frequently encountered them: at work, while doing errands, while participating in clubs and other voluntary organisations. In many countries, an obligation for men to help defend the country against military aggression was also part of the social contract. Indeed, conscription only works if it is part of the social contract. In Finland, the country that most successfully uses mandatory military service for men, conscription also enjoys enormous support among the population; in 2022, 82 per cent.[7]

In the past three and a half decades, even more countries have moved towards liberal democracy, at various paces and with various degrees of passion. The most significant push towards liberal democracies arrived in the late 1980s and early 1990s, with countries emerging from communist rule behind the Iron Curtain. When citizens of Poland, Czechoslovakia, Hungary, and other Warsaw Pact countries shook off the communist regimes imposed on them, they knew that they too wanted liberal democracy as their political system, and they knew what it should look like: free and fair elections; a benevolent, competent and transparent state apparatus; a well-informed citizenry educated to take personal responsibility but able to rely on the state in case of extreme hardship; freedom of expression as exercised both by citizens and by media in its different forms. They wanted societies that operated through democracy, the rule of law, even market economies, and in which that system was based on citizens' consent.

Today several dozen of the 210 countries and territories monitored by Freedom House in the organisation's Freedom Index – including countries as geographically distant as Germany and Ghana -- rank as free.[8] There are, of course, significant variations in their implementation of liberal democracy: Cape Verde is not the Czech Republic. The fundamental idea of it comprising empowered citizens and a benign state (whether it is large or small) has, however, guided each country's implementation of the social contract.

These recent decades' expansion of democracy has, however, been accompanied by the growth of mobile telephony, the internet and more recently social media. As recently as 2005, there were slightly more than one billion internet users worldwide; by 2022, the number had soared to 5.3 billion.[9] The internet and technologies linked to it – including hardware such as mobile phones and software-based services like social media – have done considerable good in allowing citizens to publicly express their views on virtually any subject. This has been an extremely empowering experience for citizens, who had been used to only being able to express their opinions through elections, letters to the editor or in conversations with friends, family and acquaintances. Even though this chapter concerns liberal democracies, it is worth noting that the internet and social media allow even residents of authoritarian states some degree of freedom to express themselves in public.

But, without an agreement in place regarding how societies should re-arrange themselves against such fundamentally transforming technology, the internet and social media have also poisoned the agora and fuelled social fragmentation. Before the arrival of modern communications technologies, understanding information was infinitely easier because the information arrived in front of citizens' eyes and ears evaluated by journalists and other professionals. To be sure, journalists' assessment was not always perfect and they, like everyone else, had personal biases that occasionally influenced their judgement, but by and large, citizens could trust that the information delivered to them by media other than word of mouth was trustworthy. Word-of-mouth exchanges, of course, were just that, limited in their reach and thus their influence. Today, by contrast, citizens are not just recipients of endless information: they are also megaphones, but ones mostly untrained on how to assess information and a result likely to share incorrect information and even fabrications. The arrival of Generative AI tools such as ChatGPT will further exacerbate this information anarchy, since these robots produce convincing-sounding copy without, however, guaranteeing its accuracy.

In the past several years, many citizens of such societies have also gone beyond taking the privilege of free speech for granted: they have become contemptuous of liberal democracy. Mostly unbeknownst to themselves, they have withdrawn from the social contract. Anti-vaxxers have decided to not just disbelieve public-health experts but in many cases to attack vaccination sites and even healthcare workers. Others launched online harassment campaigns against doctors and clinics.[10] QAnon supporters, in turn, have repeatedly harassed politicians, journalists and others they believe to be part of the secret cabal ruling the world.[11] Most infamously, citizens unwilling to accept Joe Biden's victory in the 2020 US presidential election stormed the US Congress, where ratification of his victory was about to take place, and attempted to thwart it. They failed in this undertaking, but it cost the lives of five people.[12] In January 2023, supporters of Brazilian presidential candidate Jair Bolsonaro – similarly believing that he had won the presidential election – stormed and vandalized the presidential office.[13] If enough citizens choose to oppose institutions put in place by popular consent, such institutions cannot survive. The United States today portends a liberal democracy at risk of becoming ungovernable because its social contract has decayed.

Another trend has also been taking place, a less obvious but equally influential one: Western societies' decline in civic engagement. In his landmark 2001 book *Bowling Alone*, Robert Putnam painstakingly documented the decline in civic engagement in the United States.[14] Between the 1950s and the 1990s, the share of Americans who attended club meetings had dropped dramatically, as had the share who had regularly ate dinner with their families or had friends over. All this, Putnam pointed out, had led to a significant decline in "social capital", the fabric that holds societies together.

Since then, civic engagement has continued to decline, not just in the United States but across the industrialised world. When social media platforms, with their easy-access bubbles of likeminded people, arrived, they capitalised on the decline in civic engagement by offering a speedy way of interacting with others, albeit in an artificial way. Indeed, on social media users can interact with others without the hassle involved with real-life engagement: travelling to meetings, speaking with people. In addition, with the exception of Finland and a few other countries that ask their men (and sometimes women) to serve in the armed forces, today liberal democracies do not ask their citizens to contribute to society in any way other than the most rudimentary one of paying taxes and obeying laws.

It should come as no surprise that high-speed internet has further accelerated the decline in civic participation. In 2022, Fabio Sabatini, Mattia Nardotto, Tommaso Reggiani, and Andrea Geraciat established that fast internet substantially displaced social capital in the UK. 'After broadband take-up, civic and political engagement started to systematically decline with inhabitants' proximity to the network node serving the area, i.e. with the speed of the Internet connection. Time-consuming activities oriented to the pursuit of collective welfare, such as engagement in associations, suffered the most from broadband penetration,' the researchers reported. In statistical terms, their investigation found that a '1.8 km reduction in respondents' distance from the local exchange, resulting in a faster connection, caused a 4.7% decline in the likelihood of participation in associational activities between 2005 and 2017. For political parties, broadband availability caused a statistically significant 19% reduction in the probability of involvement. For volunteering associations, the likelihood of people participating in these organisations reduced by 10.3%.'[15] Broadband causing a one-fifth decline in participation in political parties and a one-tenth decline in volunteering: these figures ought to worry not just politicians and social leaders but everyone concerns about the state of the social contract. The more modern communications technologies continue to develop and the more space they occupy in citizens' lives, the more they will erode the remnants of existing social contracts. How are citizens expected to co-exist in an era that will see artificial intelligence (AI) and the Internet of Things present in most parts of their daily lives? It has not been established.

Such continued decline in social capital and civic engagement is highly likely to lead to further societal fragmentation and accelerated decay of the social contract. Countries are already seeing a fait accompli, in which citizens take the communal good for granted but do not contribute to it or, worse, harm it through their actions. In the case of the US Capitol attack, police officers and the National Guard could eventually remove the intruders, but the harm to US democracy lasted. Indeed, in Freedom House's 2022 index the United States has slid below peer liberal democracies on key democratic indicators including executive elections and freedom from improper political influence.[16]

Liberal democracies need a new social contract, one addressing today's digitally powered and highly individualised age. As with all social contracts, this needs to be a contract that can be supported by all parts of society; and like other social contracts, this would not be a government diktat but a civic rules-of-engagement manifesto of which people of all walks of life could take ownership. To be sure, not all citizens will want to make even a small contribution to society: their modus operandi is instead to issue a constant stream of complaints about their society even as they benefit from its communal services. It, however, stands to reason that most citizens are willing to adhere to a social contract that contains both rights and obligations for them because they want their societies to operate with some degree of societal harmony, both because this brings better quality of life and because it is mutually beneficial. Indeed, having seen the shocking harm the decay of an existing social contract can cause, they are likely to support society-wide agreement on how a country's different parts can co-exist beyond the bare minimum of obeying the same laws and paying taxes to the same government.

In January 2022, the World Economic Forum concluded that countries need a new social contract. 'A social contract fit for contemporary society should address three fundamental challenges. First, familiar elements of the safety net, such as social insurance and pension benefits, need to address a new set of circumstances, such as the need for people to reskill during much longer working lives. Second, social contracts must be relevant in a world being reshaped by technological revolutions, and the transition to a clean energy economy. Third, a modern social contract must tackle the inequality and exclusion that plague societies in all corners of the world,' the WEF explained and listed five areas to be included: stakeholder capitalism; skill development and career pathways; economic security and mobility; a just and inclusive transition to net zero; and responsible use of technology.[17] The areas listed by the WEF are not wrong, but they hardly constitute a social contract: they are various policy areas in which governments can pursue solutions in cooperation with private-sector partners.

A social contract is, as we have seen, instead the tacit agreement among citizens and between citizens and the government governing how the citizenry can co-exist with the right to free speech and without descending into anarchy. A social contract fit for the digital age must continue to include the expectation that citizens will contribute to the common treasury, whose funds the government will judiciously use. It must also, once again, include agreement on how citizens use freedom of speech and freedom of assembly, and under what conditions the government should curtail such activities for the benefit of the common good. Today, however, there is no such agreement. That is why governments, social media platforms and citizens alike struggle so mightily to discern what the rules of engagement should be.

How can governments and the citizenry go about forming a new social contract? Liberal democracies would do well to start by asking – perhaps in townhall-style forums and certainly in school and university classrooms -- what citizens think citizens should do for their country. They would be certain to receive large numbers of wise and insightful suggestions. Especially in an era of citizens empowered by communications technology, academics and policymakers do not have a monopoly on ideas for ways to improve societal co-existence. If consulted in this manner, citizens might propose that a new social contract should involve not just the right to free speech but the obligation to consider the consequences when one engages in free speech. They might propose that liberal democracy's long-standing elected seats of power be joined by other, non-legislative, forums where citizens can express their opinions: regular, consultative town hall meetings. They might propose that a social contract should include not just a right for citizens to access society's communal goods but to contribute to it beyond the rudimentary paying of taxes and obedience to the law. Such contributions could involve whatever society deemed necessary at any given time. Participation in war will certainly not be necessary, but assisting frail and elderly citizens certainly is.

A fundamental part of a future social contract, though, must be citizens' duty to understand information. The reason that today's citizens so often believe falsehoods, spread falsehoods, and erroneously attack one another and societal institutions is that they lack the knowledge necessary to assess and verify the enormous amounts of information now available to them. Such information literacy will become more crucial still as information continues to grow and disinformation and misinformation along with it. In January 2023, for example, an image of a Parisian police officer in ridiculous-looking hat was enthusiastically shared on social media, including by national-security experts, who not only failed to spot that the image was a deep-fake but who also failed to realise that by sharing it they were helping hostile states' campaigns discrediting Western institutions.[18]

There is no shame in not being 21st century information-literate; on the contrary, most citizens are not, and the fewest citizens can acquire such skills on their own. Yet understanding information is indispensable in a liberal democracy. Most citizens would, I posit, agree to a social contract where it is their responsibility to become literate about information and societal institutions' responsibility to provide such training. If citizens do not discuss on the basis of the same facts, their country will become ungovernable.

Indeed, as technology continues to advance, continuous training more widely should also be part of the social contract. Today many employers and indeed many governments offer continued education throughout citizens' professional lives, but this could be codified in a social contract. That would also allow the many workers who feel left behind by automation and offshoring to feel that they, too, have an active role in society. It is noteworthy that a large share of the people who stormed the US Capitol were people who felt excluded or marginalised by society.

A social contract, though, must involve everyone, because all groups of citizens have rights and obligations. Indeed, an acceptable level of co-existence harmony in a liberal democracy requires that all parts of society agree on a minimum set of rules of engagement: a social contract.

Conclusion

Social contracts are not written agreements: they are a set of rules of engagement that citizens learn and adopt as they grow up. The digital age – launched through mobile phones and the internet and advancing through AI and the Internet of Things – has so fundamentally changed citizens' engagement with one another and with societal institutions that a new social contract is necessary. Because a social contract is not a written document, and because the digital era has created an environment of highly empowered and vocal citizens, governments would be well-advised to consult the citizenry on what the new rules of engagement ought to include. After soliciting citizens' input through public-awareness campaigns, the government of any given country could appoint a commission comprising legislators, technology experts, academics in subjects including history, media and sociology, and representatives from among the citizens who submitted suggestions. This commission would then be tasked with formulating rules of engagement – the new social contract – that could then be shared with the population in the same way as other public-awareness campaigns. Citizen involvement would be crucial not just for democratic legitimacy and to ensure a wide range of views, but because citizen engagement at the idea stage generates more citizen commitment to the final product.

Endnotes

1 Brians, P. (n.d.). Rousseau, Jean-Jacques: The Social Contract (1762). Retrieved from https://brians.wsu.edu/2016/11/04/rousseau-jean-jacques-the-social-contract-1762/

2 Ibid.

3 Internet Encyclopedia of Philosophy. (n.d.). Social Contract Theory. Retrieved from https://iep.utm.edu/soc-cont/

4 Rousseau, J. J. (1762). The Social Contract. Retrieved from https://www.earlymoderntexts.com/assets/pdfs/rousseau1762.pdf

5 Ibid.

6 USHistory.org. (n.d.). Ask Not What Your Country Can Do For You. Retrieved from https://www.ushistory.org/documents/ask-not.htm

7 Finland Ministry of Defence. (2022). Finländarnas åsikter om utrikes- och säkerhetspolitiken, försvaret och säkerheten, december 2022 (p. 38). Retrieved from https://www.defmin.fi/files/5569/PFI_December_2022.pdf

8 Freedom House. (2022). Freedom in the World 2022. Retrieved from https://freedomhouse.org/report/freedom-world/2022/global-expansion-authoritarian-rule

9 Statista. (2022). Number of internet users worldwide from 2005 to 2022. Retrieved from https://www.statista.com/statistics/273018/number-of-internet-users-worldwide/

10 Paunova, P. (2022, January 19). I'll Kill You!: COVID Anti-Vaxxer Attacks Doctor In Bulgaria. RFE/RL. Retrieved from https://www.fiercehealthcare.com/practices/anti-vaxxers-attack-pediatric-practice-we-decided-to-take-a-stand-says-doctor

11 Fu, A. (2021, February 10). Embedded within a mass delusion: The challenge of reporting on Qanon. Poynter. Retrieved from https://www.poynter.org/reporting-editing/2021/embedded-within-a-mass-delusion-the-challenge-of-reporting-on-qanon/

12 Evelyn, K. (2021, January 8). Capitol attack: the five people who died. The Guardian. Retrieved from https://www.nytimes.com/2021/01/11/us/who-died-in-capitol-building-attack.html

13 Faiola, A., & Dias, M. (2023, January 8). Assault on presidential palace, Congress challenges Brazil's democracy. Washington Post. Retrieved from https://www.washingtonpost.com/world/2023/01/08/bolsonaro-invade-congress-lula/

[14] Putnam, R. (2001). Bowling Alone. Touchstone Books. Retrieved from http://bowlingalone.com/

[15] Sabatini, F., Nardotto, M., Reggiani, T., & Geraci, A. (2022, February 12). Faster Internet displaces social capital in the UK. Centre for Economic Policy Research. Retrieved from https://cepr.org/voxeu/columns/faster-internet-displaces-social-capital-uk

[16] Freedom House. (2022). Freedom in the World 2022 (p. 9). Retrieved from https://freedomhouse.org/sites/default/files/2022-02/FIW_2022_PDF_Booklet_Digital_Final_Web.pdf

[17] World Economic Forum. (2022). Why we need a new social contract for the 21st century. Retrieved from https://www.weforum.org/agenda/2022/01/a-new-social-contract-for-21st-century/

[18] [Tweet]. Retrieved from https://twitter.com/Rossmac212/status/1610749990737002497