Deutsche Bank
Research

EU Monitor
Digital economy and structural change

Digital politics

August 22, 2019

AI, big data and the future of democracy

Author
Kevin Körner
+49 69 910-31718
kevin.koerner@db.com

Editor
Barbara Böttcher

Deutsche Bank AG
Deutsche Bank Research
Frankfurt am Main
Germany
E-mail: marketing.dbr@db.com
Fax: +49 69 910-31877

www.dbresearch.com

DB Research Management
Stefan Schneider

For billions of people, the digital transformation has brought enormous benefits and convenience. Yet, policymakers and market participants will likely only be able to understand the full economic and political implications in hindsight. This is a major challenge when it comes to addressing the risks and opportunities of technology for democratic institutions and processes.

Digital technology can be used in the service of liberal or authoritarian societies, strengthening both government accountability and repressive capabilities. It has led to unprecedented access to and exchange of information, and it has amplified the spread of misinformation, echo chambers and propaganda, thereby possibly contributing to rising populism and the polarization of democratic societies.

Users across the globe enjoy ‘free’ services in the data economy, but underlying business models and a concentration of influence and wealth have raised pressing questions regarding privacy, data ownership and targeted manipulation for both economic and political purposes. Authoritarian states have quickly learned to use surveillance technology, artificial intelligence and mass data to their advantage in order to gain domestic control and to erode democratic societies abroad.

For democracies whose cohesion is based on the sovereignty and consent of their citizens, this represents an unprecedented challenge. How democracies approach this challenge will likely be a key factor in their performance, given intensifying competition among political systems.

Governments are being required to update regulations, competition rules and supervision in order to fulfil the new requirements of the global digital economy. Companies are being required to assure that their business models and products are compatible with users' constitutional rights and the integrity of democratic institutions and processes. Citizens are being required to be ‘digitally literate’ so as to better understand the algorithms/designs behind apps/devices and underlying data economy mechanics.

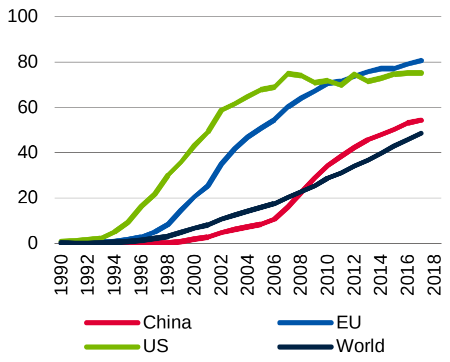
We believe that democracies need an informed dialogue on data and technology ownership, one that discusses how to share the benefits of AI and automation, and how to prevent increasing asymmetries in wealth and power from destabilizing their foundations. We also believe that competitiveness in key technologies will be crucial for maintaining economic prosperity and public support for democratic order.

The EU has taken a front seat in addressing the challenges posed by the digital transformation as they relate to citizens and society as a whole. It has become a global role model for fighting disinformation and for setting legal and ethical standards for data protection and AI development.

AI, big data and the future of democracy

Surge in global connectivity 1

Internet users (% of population)



Source: World Bank from World Telecommunication/ICT Development Report and database

Democracy needs to be protected. Citizens growing up in liberal democracies often take their constitutionally protected rights and freedom for granted, and they tend to assume that nothing can shake this basic order. However, others have experienced life under authoritarian or totalitarian structures and are more sensitized to the issue. They have learned that democracy can never be taken for granted. In fact, democracies like those that have prevailed over the last 30 years are the absolute exception in human history.

The separation of powers, independent courts and freedom of the media are democracy's protection mechanisms against authoritarian attempts to overthrow and undermine its foundations. However, in recent years, the potential fragility of these mechanisms has been demonstrated in several democratic countries around the world, including some within the European Union.

This serves as a warning that democratic institutions cannot function properly if alone. They depend on informed and committed citizens, and their political representatives. In this context, the digital transformation of the last two decades has increasingly presented itself as a double-edged sword.

Technology by itself is politically neutral. It can be used in the service of liberal or authoritarian societies, and can strengthen both government accountability and repressive capabilities. However, this does not mean that the state of technological development is immune from providing advantages to one or another form of political or economic organization. Indeed, technology is one of the driving factors of human history. But how it will shape societies and political systems depends on its implementation through companies and governments, and its adaption through citizens.

Benefits for billions. The benefits of the digital transformation over the past years for human communication and organization are undoubted. People enjoy access to information that was unimaginable just a few decades ago and the possibility to exchange and coordinate themselves worldwide in a matter of seconds. For billions of people, the digital transformation for which the smartphone is synonymous has brought enormous benefits and convenience. This has enriched the societal discourse through new forms of multilateral communication. Social media such as Facebook and Twitter have become standard tools for citizens, representatives and governments to reach out to each other and exchange views, opinions and policy proposals.

Early hopes for a technology-driven wave of democratization. In the nineties, at the dawn of the World Wide Web, there was great hope that global connectivity and rapid technological progress would lead to a new wave of democratization. It was assumed that the wider technology is distributed, the more this would strengthen democratic control through citizens and the accountability of governments.[1] During the Arab Spring at the beginning of this decade, it still looked as if this promise would be fulfilled, when state censorship and assembly bans in authoritarian states were circumvented by social media.

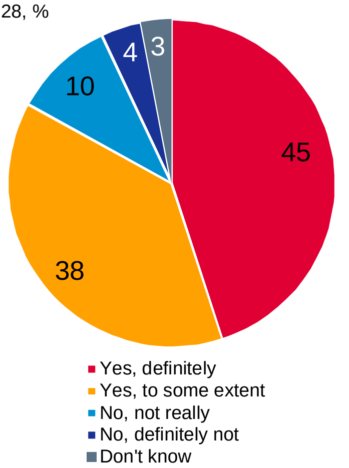
The dark side of technology. It has taken several years after the initial euphoria and broad adoption of key digital technologies that the challenges posed by these technologies have become gradually recognised by individuals, civil rights groups, governments and society as a whole. In particular, the scandals surrounding Cambridge Analytica and Facebook in connection with the Brexit referendum and the US presidential elections in 2016 have shown that digital

[1] Foreign Affairs (February 12, 2019). Does technology favor tyranny?

technology can also be used in established democracies to deliberately manipulate voters and distort the political discourse.

EU survey: Fake news and democracy 2

EU28, %



Survey: "In your opinion, is the existence of news or information that misrepresent reality or is even false a problem for democracy in general?" (EU28, %)

Source: Flash Eurobarometer 464 (April 2018)

The technological leap of the last decade took place so rapidly that both policymakers and market participants often understood its full implications only in hindsight. This certainly is one of the major challenges for legislators and regulators on the question of how to deal with the risks of technology for democratic institutions and processes.

The demands on individuals to filter and critically question the daily flood of information have increased drastically. At the same time, the rapid integration of social media platforms into all areas of users' lives has created unprecedented opportunities for targeted, individualized, automated and often unnoticed influence.

Authoritarian states have also quickly learned to use surveillance technology, mass data and artificial intelligence to their advantage, both for domestic control as well as the erosion of democratic societies abroad.

An unprecedented challenge to democracy. For a social order whose cohesion is based on the sovereignty and consent of its citizens, this represents an unprecedented and potentially vital challenge. How democracies approach this challenge will be a key factor for their performance in the intensifying competition of political systems.

The experience of the last few years and mounting anecdotal evidence helps to identify some key areas where digital technology can threaten to undermine and destabilize democracy:

— Misinformation, echo chambers, and targeted manipulation

— Tectonic shifts of financial and political power in the data economy

— Loss of privacy and user sensitivity

— Persuasive technology and social media addiction

— Erosion of civil rights through algorithmic bias

— Mass surveillance and the strengthening of authoritarianism

— Impact of AI and automation on competitiveness and the support for democracy

Misinformation, echo chambers, and targeted manipulation

The most visible impact of the digital transformation of the last two decades on politics is in communication and the exchange of information between individuals and societies as a whole. Propaganda, disinformation and manipulation have been essential political tools since the dawn of mankind. But paramount connectivity, increasingly cheap (mobile) computing and the data availability of the last few years allowed for an unprecedented and coordinated spread of misinformation and individualized manipulation on a new level.

Policymakers and societies have started to understand some of the most pressing implications:

— Coordinated misinformation on a mass scale

— Micro-targeting of voters

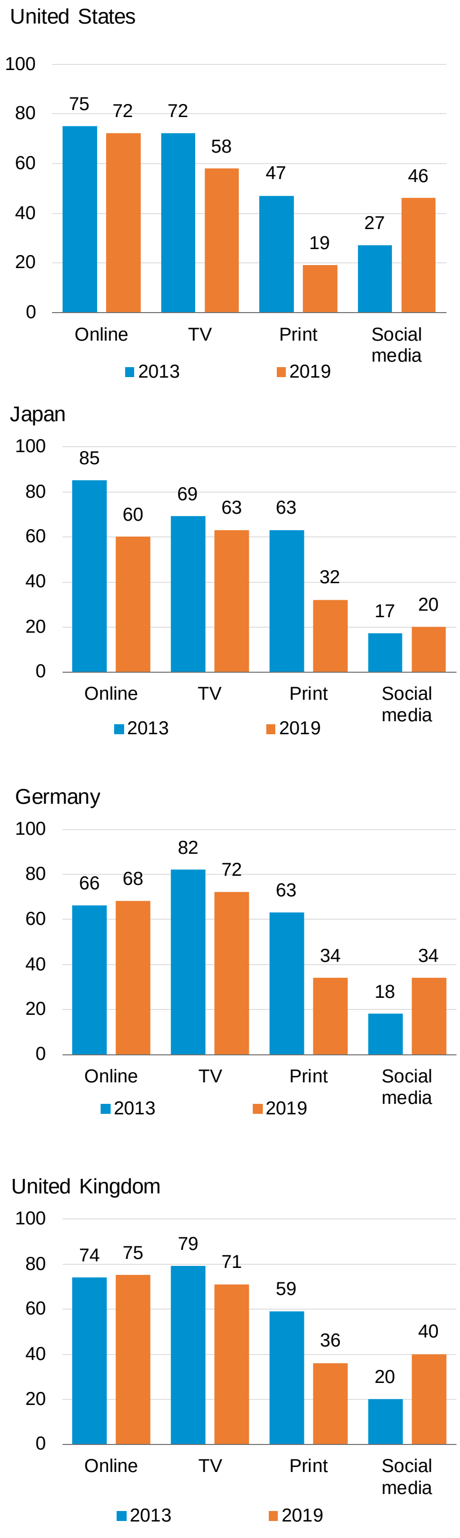
— Polarization of the public dialogue in democratic societies

— Hybrid warfare and distrust of democratic institutions and governments

— Tightening state control of information flow and public opinion in authoritarian societies

Online dominates users' news consumption in most countries 3

Source of news, %



Source: Reuters Institute Digital News Report 2019

Disruption of information dominance and the polarisation of society. In democratic societies, a major challenge lies in the disruption of the traditional communication landscape previously dominated by established media through digital and multilateral communication and social media platforms. In principle, the additional supply of alternative, multilateral and mainly free information and news content can be seen as an enrichment of the political debate and a tool to empower citizens, unveil corruption and to hold governments accountable.

However, the lack of information scrutiny that often characterizes these platforms and their inherent tendency to algorithmically reinforce existing opinions among users has led to the spread of coordinated misinformation and propaganda, and the creation of digital filter bubbles or “echo chambers” that can polarize society and undermine the public dialogue.

Shift to ‘free’ online media spurs sensationalism. As an increasing share of people globally has shifted their information consumption to online media, news feeds and social media platforms, these have become an important factor in the political process. This change in news consumption habits has also led to an increasing spread of sensationalism to politics, as the business model of platforms and online journalism tends to favor emotion over fact-based content.

The heightened political division and rise of populism in democratic societies, as well as the fragmentation of party landscapes in recent years, coincides with the rise of social media and universal connectivity, and might at least be partly attributed to this development.[2]

New dimensions of cyber conflict and authoritarian control. From a geopolitical perspective, ‘hybrid warfare’ has gained growing importance through new and increasingly cheap technologies. Authoritarian governments with an agenda to discredit and undermine democratic counterparties and manipulate foreign electorates exploit the access to free communication in democratic and liberal societies through an open internet. At the same time, they restrict their own citizens' access to information from abroad by ring-fencing and censoring the internet at home while using online media and platforms to control and steer public opinion.

The toolbox of influencing users and citizens domestically and abroad includes the spread of factually incorrect or highly misleading information through social ‘bots’, software applications that operate through automated social media accounts and that mimic human behavior in order to influence public sentiment. Rapid progress in AI technology also enables increasingly sophisticated ‘deep fakes’, i.e. the manipulation and forgery of audio and video content, allowing the spread of misinformation and propaganda that goes far beyond chat comments and faked news articles.

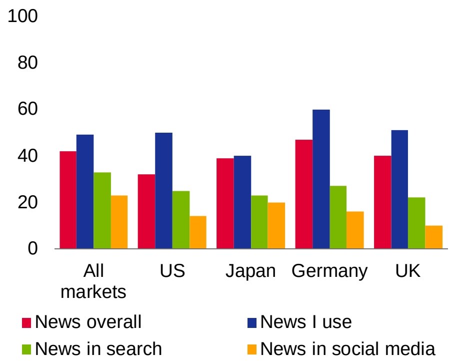
Loss of trust. The continuous spread of conspiracy theories and other factually incorrect or highly biased information undermines citizens' ability to identify ‘objective’ or shared truth. This can lead to a distrust of all media, fatalism and disengagement among parts of the population, severely damaging the societal dialogue and amplifying political divisions.[3] This is particularly challenging in view of new developments and complex issues, where people cannot refer to

[2] European Parliament (2019). Polarisation and the use of technology in political campaigns and communication.

[3] Deibert, Ronald J. (2019). The road to digital unfreedom: Three painful truths about social media. Journal of Democracy.

Low trust in news a global phenomenon 4

Trust in news, % of users

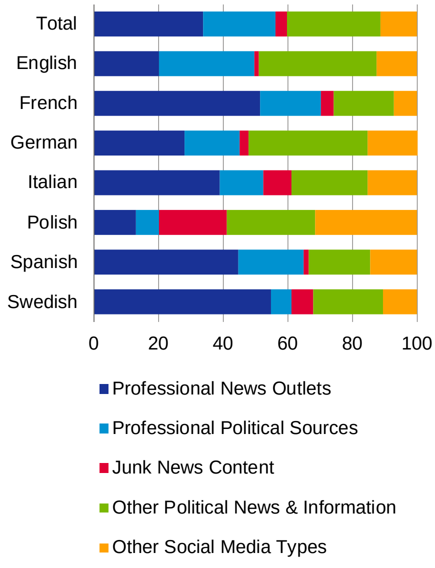


All markets: 24 from Europe, 7 from Asia, 6 from the Americas, 1 from Africa

Source: Reuters Institute Digital News Report 2019

Junk news in EU Parliament elections 5

Types of political news/information shared over Twitter, %



Source: Oxford Internet Institute, Junk News During the EU Parliamentary Elections (2019)

their own (collective) experience.[4] This loss of trust serves authoritarian regimes, which aim to destabilize democratic societies that question their own claim to unchecked power as well as delegitimize the liberal democratic model in the eyes of their own populace as dysfunctional, hypocritical and decadent.

The so far most prominent cases of foreign interference and voter manipulation through social media have been around the 2016 US presidential elections and Brexit referendum in the UK.

Russia and the 2016 US presidential elections. In the US, the "Mueller Report" released earlier this year found that "the Russian government interfered in the 2016 presidential election in sweeping and systematic fashion." According to the report, the Russian-based "Internet Research Agency" had the ability to reach out to millions of US social media users through social media accounts (Facebook, Twitter, Instagram) that pretended to be controlled by US activists. The social media campaign aimed to "provoke and amplify political discord in the United States" and "favoured candidate Trump". The second major campaign was a hacking operation by Russian intelligence in order to release "hacked materials damaging to the Clinton Campaign".[5.] Also, for the 2020 US elections, the FBI Special Council Mueller warned of an increased risk of Russian interference.[6]

The Facebook-Cambridge Analytica scandal. In a settlement with the Federal Trade Commission this July, Facebook was fined a record USD 5 bn over privacy breaches, including the 2016 Cambridge Analytica scandal, and had to agree to new privacy controls. Critics say this fine had not gone far enough and that it remained unclear when Facebook became aware of Cambridge Analytica's abuse of the data of millions of Facebook users for psychometric profiling and micro-targeting ahead of the 2016 US presidential elections.[7] Recently, a former Cambridge Analytica official confirmed that the data analytics firm also worked for Leave. EU and the UKIP parties ahead of the 2016 Brexit referendum, a claim that these repeatedly denied.[8]

Political social media abuse a global phenomenon. The 2016 scandals are no isolated events, however. The impact of social media on elections and the political discourse has become a global phenomenon. As a most recent example, related to the Hong Kong protests, Twitter and Facebook have removed Chinese accounts in order “to block what they described as a state-backed Chinese misinformation campaign”, according to the BBC.[9] The global dimension was illustrated earlier already by the misuse of Facebook and WhatsApp to circulate disinformation, hate speech and propaganda in India and Brazil, two of the largest democracies in the world[10]. It has also become evident that attempts to manipulate voters and the public through trolls, bots and targeted manipulation particularly come from the political fringes.[11]

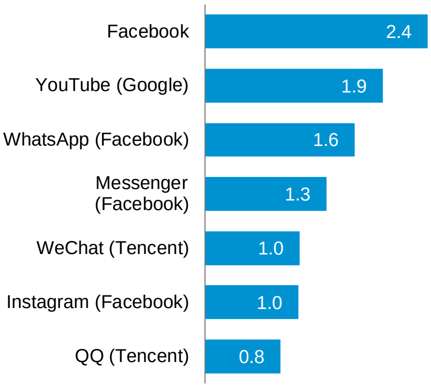
Europe also in the focus. Also, in Europe, junk news and traffic manipulation to influence voters and public opinion have become a common phenomenon. This includes national elections in Germany, France and Sweden, as well as the

[4] Schneider, Stefan (2017). Vox populi, vox dei or maybe not? Deutsche Bank Research. Germany Monitor.
[5] US Department of Justice (2019). Report on the investigation into Russian interference in the 2016 presidential election.
[6] Financial Times (July 25, 2019).
[7] The Hill (August 4, 2019).
[8] Politico (July 30, 2019) and The Guardian (July 30, 2019).
[9] BBC (August 20, 2019).
[10] BBC (April 6, 2019) and BBC (October 24, 2018).
[11] European Parliament (2019). Polarisation and the use of technology in political campaigns and communication.

Catalonia referendum in Spain and yellow vest protests in France, according to a research project organized by Oxford University.[12]

Global reach of social media 6

Monthly active users in billions, end-2018 / Q1 2019



Sources: Company reports and websites, DataReportal by Hootsuite and We are social, Deutsche Bank Research

Policymakers have started to react to the challenge. Ahead of the European Parliament elections in May, the European Commission outlined an action plan to counter disinformation, including the agreement on a self-regulatory "Code of Practice on disinformation" with major social networks.[13] Facebook opened a 'war room' to prevent interference in the EU elections through its platform. But while the spread of misinformation and propaganda in the EU elections appear to have been far from the epidemic dimensions observed in some other parts of the world, there is still sufficient evidence that online users were exposed to deliberately misleading and deceptive information, bots and fake accounts.[14]. The European Commission also published a report saying that it found evidence of "continued and sustained disinformation activity by Russian sources aiming to suppress turnout and influence voter preferences."[15]

This shows that the fight against disinformation, hate speech and automated propaganda in democracies remains an ongoing challenge, in particular regarding the question of how an open society can address the issue without falling into censorship and violating the fundamental right of freedom of expression.[16]

Tectonic shifts of power and influence in the data economy

The disruption of traditional ways of communication and information exchange described above is a consequence of the rise of a new and powerful business model, often described by observers in partly overlapping but not synonymous terms as:

'platform', 'data', 'attention' or 'surveillance' economy

Tech companies that provide (apparently free) services to their users, such as online searches, peer communications, games and other entertainment, become gateway keepers to advertisers by providing access to users' attention and data to optimise ad placements. As has been shown by the dramatic rise of the market value of companies such as Google and Facebook (which together command a 60% share of the US digital ad market), the monetisation of user access and data is vastly profitable.[17]

Big techs' exclusive control of massive data gives them an enormous advantage not only in their respective market segments but also in the development and training of AI, further strengthening their market position in established markets and providing them with a head start in new ones.

The age of 'surveillance capitalism'. Harvard economist Shoshana Zuboff speaks of the beginning of a new era, the age of "surveillance capitalism". According to her, the economics of scale and scope in the platform economy have brought about a rapidly increasing concentration of data, knowledge, financial power and control of communication channels in the hands of a small technology elite.[18]. For Zuboff, this results in a rapidly increasing social

[12] Oxford Internet Institute (2019). Junk news during the EU parliamentary elections: Lessons from a seven-language study of Twitter and Facebook.

[13] European Commission (2019). Tackling online disinformation.

[14] Politico (May 23, 2019).

[15] Deutsche Welle (June 14, 2019).

[16] European Commission (2019). Countering illegal hate speech online – EU Code of Conduct ensures swift response.

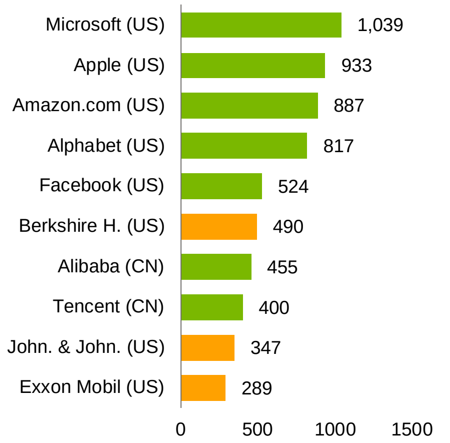
[17] VOX (February 20, 2019).

[18] Zuboff, Shoshana. (2019). The age of surveillance capitalism.

asymmetry of economic and political influence.[19] Her assessment is shared by Israeli historian Yuval Noah Harari. Harari considers the increasing tribalism in politics and the strengthening of authoritarian and populist currents in democratic societies as closely linked to the technological developments of our time. He fears that the influence of the public on the political process could dwindle unnoticed, while supposedly free decisions and elections could at some point provide only a democratic facade.[20]

10 largest global companies - 7 tech giants from US and China 7

Market capitalisation (USD bn)



Source: Bloomberg Finance LP (accessed on August 19, 2019)

Tech insiders warn about their own creations. But technology warnings not only come from academics, luddites and general critics of capitalism. Some of the most outspoken critics have been instrumental in the technological developments of recent years. For Tristan Harris, formerly responsible for design ethics at Google, billions of people are increasingly influenced in their decisions and views by a handful of companies, with far-reaching consequences for the democratic discourse.[21] James Williams, a former Google product strategist, wonders whether democracy can survive the technological age at all. He speaks of an "attention economy", in which algorithms compete for users' time, placing sensational and emotionally appealing content over the rational and fact-based. For Williams, this also increasingly applies to politics.[22]

Calls for increased scrutiny of big techs to protect democracy. Some commentators see the Cambridge Analytica scandal as a warning that technology owned by some of the wealthiest members of society can be used to systematically manipulate the populace in order to establish a 'managed' democracy serving mainly the narrow interests of a 'global plutocracy'.[23] Also, among policymakers, there are some who propose a break-up of tech giants in order to mitigate their growing accumulation of economic and political influence, including US Senator and presidential contender Elizabeth Warren from the Democrats.[24] Others go less far by proposing tighter regulation and supervision of the data economy. Also, the Trump administration has increased the scrutiny of tech companies, as the Justice Department opened an investigation into potential anticompetitive practices.[25] The heightened discussion on how to address this challenge illustrates the vast societal and political impact of digital companies over the last years.

Loss of privacy and user sensitivity

The spread of the data economy has become almost universal as cheap access to smartphones and free content have made online behaviour more or less independent from people's financial, ethnic, religious and political background. At the same time, users across borders and political systems have quickly got used to trade convenience, access to peers and social affirmation, against their own, often highly personal, data.

[19] Zuboff, Shoshana (2016). The secrets of surveillance capitalism. Frankfurter Allgemeine Zeitung. March 5, 2016.
[20] Harari, Yuval Noah (2018). Why technology favors tyranny. The Atlantic. October 2018.
[21] Harris, Tristan (2017). How a handful of tech companies control billions of minds every day. TED2017.
[22] The Guardian (2017). Our minds can be hijacked: The tech insiders who fear a smartphone dystopia. October 6, 2017.
[23] Cadwalladr, Carole (May 7, 2017). The great British Brexit robbery: How our democracy was hijacked. The Guardian.
[24] Los Angeles Times (March 21, 2019).
[25] Reuters (July 23, 2019).

Users have quickly got used to being observed almost around the clock ... not by Orwell's Big Brother, at least not in democratic societies. But by our all-purpose computer in the pocket, supplemented by other high-tech products such as smart TVs, smartwatches, fitness trackers or virtual assistants. Cookies, tracking tools and social logins allow the synchronisation of data on users' online behaviour across platforms, websites and devices. These give constant information about our whereabouts, behaviour, attitude, mood, preferences and social life. It enables companies in the data economy to create accurate personality profiles and behavioural predictions, and thus exert targeted influence or 'micro-targeting'.

Privacy versus free services. Many users feel uncomfortable about the use of their private data. But as a survey from the US suggests, the majority might still prefer 'free of charge' services over better data protection.[26.] This has also been illustrated in the aftermath of the Cambridge Analytica scandal, which shows no substantial or sustained impact on the social media behaviour of most users.[27]

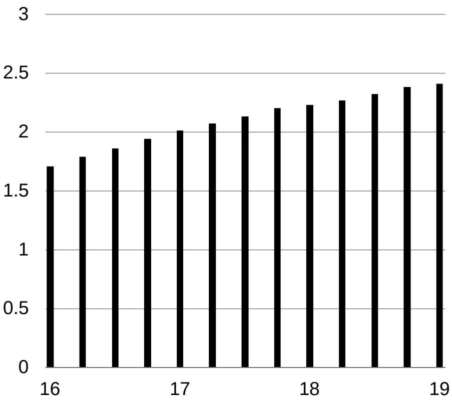
A trade of personal data against 'free' services should in principle be considered users' individual choice in an open market, as long as they are well informed about the implied conditions. However, several factors put that voluntariness and consent into question. Many services and devices strongly limit the freedom of choice users have in controlling their data and protecting their privacy. Apart from digital abstention, it is almost impossible to avoid being tracked online on a regular basis and to avoid the collection of personal data. Disclaimers and terms of use regarding privacy are frequently formulated intentionally vague, broad and lengthy, which discourages users from going through them in depth.[28] As a consequence, users are frequently not aware of the extent to which they allow service providers to access, process and proliferate their data. Users with privacy concerns also often see no alternatives to major social networks and messaging services to remain connected to their families, friends and peers, and might therefore reluctantly accept the implied loss of privacy.

Europe leads the response on privacy. In Europe, the General Data Protection Regulation (GDPR) that went live in 2018 to give users more control over their own data has addressed many of these issues.[29] However, to ultimately reach this goal, GDPR still needs to be better linked with other EU privacy laws. In addition, it can remain cumbersome and time-consuming for users to claim their rights. Still, the GDPR is not toothless. Facebook, for example, could be facing a fine of billions of euros under the regulation.[30]

Privacy as a public good. Privacy concerns in public dialogue are primarily about user rights and the protection of their personal data. However, from a political perspective, the issue goes much further. The concentration of user data in the hands of a few large companies gives them unprecedented knowledge and access to citizens' thoughts, opinions and emotions. Based on these data, users can become subject to tailor-made attempts of behavior modification, without their awareness or explicit consent. In both democratic and authoritarian societies, this knowledge and influence can be used not only for economic purposes but also political ones. This makes the question of privacy protection and data ownership more than one about individual rights and choices, but rather one about public goods.

Steady increase of Facebook users 8

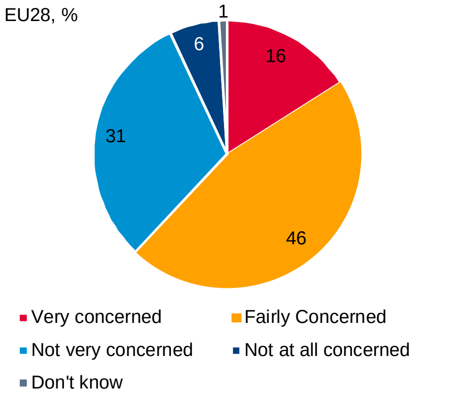
Facebook monthly active users (MAUs), bn



Source: Facebook

More than 60% of Europeans worry about their data online 9

EU28, %

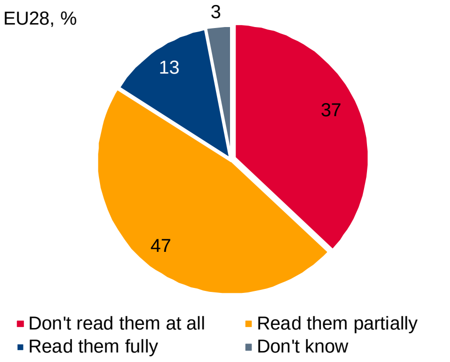


Survey: "How concerned are you about not having complete control over the information you provide online?"

Source: Special Eurobarometer 487a (June 2019)

[26] MarketWatch (Jan 19, 2019).
[27] Facebook.
[28] Business Insider (November 15, 2017)
[29] Körner, Kevin (2018). GDPR – boosting or choking Europe's data economy? Deutsche Bank Research. Talking Point.
[30] Wall Street Journal (August 12, 2019).

But only 13% read privacy statements fully 10



Survey: "Thinking about privacy statements on the Internet, which of the following sentences best describes what you usually do?"

Source: Special Eurobarometer 487a (June 2019)

Desensitization. In addition, there is a major risk to the “desensitization” of users regarding data breaches and intrusion of privacy, or “psychic numbing” as Shoshana Zuboff calls it.[31.]Users could get used to the impression that data abuse and breaches are unavoidable and that extensive data collection is the involved companies' prerogative. Users might also decide that for them the protection of privacy comes at too high a price. With a short-term time preference for ‘free’ services, they might thus not see the implied long-term costs. As they become used to private companies stockpiling and analyzing their data, they might also become less concerned about governments and authorities doing the same.

In authoritarian countries, users might not have much of a choice ... and this could also be true for democracies as well. In particular, in the ones where checks and balances are weak, this could become a major issue, where elected governments and political groups might be tempted to use these data to maintain their control, manipulate the electorate, and suppress dissent and opposition.

Persuasive technology and social media addiction

Before, we assumed online behaviour and the data sharing of users to be generally voluntary, although not necessarily always based on informed choices. However, there is some indication that some users at least might develop behavioural patterns related to their smartphones and the social media platforms they host that go to compulsion that can resemble addiction to gambling.[32.] Research on the issue is only in its infancy, often focused on adolescents and so far inconclusive.

Research published by Ofcom finds for the UK that people on average check their smartphones every 12 minutes during the waking day. According to them, 34% of people feel "cut off" without the internet, 29% "feel lost" and 17% find it "stressful".[33.] Other studies have started to show a connection between "smartphone usage and increased levels of anxiety and depression, poor sleep quality, and increased risk of car injury or death", according to Trevor Haynes from Harvard Medical School's Department of Neurobiology.[34]

Addiction by design? If social media and smartphone apps have an addictive potential, what makes the matter more concerning is that this might not be accidental. According to Nir Eyal, a former Stanford lecturer and behavioural design expert from Silicon Valley, “the products and services we use habitually alter our everyday behaviour, just as their designers intended.”[35] Companies have invested vast sums in research and talent in order to design their apps to maximize users’ attention and frequency of usage. Similar to gambling machines, small details such as the colour and display delay of Facebook's notification symbol were meticulously programmed.[36]

Dopamine-driven social-validation feedback loops. This technology is based on findings from psychology and neurochemistry, and deliberately uses our innate needs for social interaction and reciprocity. It is now understood that positive social interaction can trigger a strong dopamine rush in human brains.[37] Social networks and other apps can exploit this to modify users' desires and behaviour to increase their interaction. Sean Parker, Facebook’s founding President, calls

[31] Zuboff, Shushana. (2019). The age of surveillance capitalism.
[32] Forbes (Aug 16, 2019).
[33] Ofcom (2018). Communications market report.
[34] Haynes, Trevor (2018). Dopamine, smartphones & you: A battle for your time.
[35] Eyal, Nir (2019). Hooked: How to build habit-forming products.
[36] The Guardian (October 6, 2017).
[37] Brent, Lauren J.N. et al. (2014). The neuroethology of friendship.

Facebook's strategy to grasp the maximum of users' “conscious attention” a “social-validation feedback loop” designed to exploit “a vulnerability in human psychology" by providing users with “a little dopamine hit every once in a while”.[38]

According to Eyal, companies that form “strong habits” manage to link their products to “internal triggers”. In what he calls the "hook" model, they use the users' “daily routines and emotions” and leverage the elevation of dopamine through "variable rewards", thereby suppressing the part of the brain responsible for "reason and judgement" and activating the part associated with "wanting and desire". These “habit-forming products” tie users to the services, strengthen the trigger for the next interaction, and have thus a big competitive advantage.[39]

The science of persuasive technology. These insights are taught as ‘persuasive technology' or ‘captology' prominently at California's Stanford University, the academic heart of Silicon Valley's tech infrastructure.[40] Applied to a broad range of websites, networks and apps, this general psychological framework is supplemented with users' data in order to approach them in a tailor-made fashion.

Users might be encouraged to buy products and services, share or consume content or change their behaviour (e.g. ‘nudging' through health apps). Most importantly, they are conditioned to spend more time on the application. Revisiting the case of Cambridge Analytica and Facebook, these tools can also be used to address human fears and prejudices to modify opinions and electoral behaviour.

How does this relate to the question of technology and its impact on democracy? If the use of social media is potentially addictive, intentionally so, and not a marginal phenomenon that affects only a small share of users, the consequences for democracy could be substantial. It could mean that despite users' increasing awareness and discontent about breaches of privacy or manipulation attempts, they might not be able to change their social media behaviour. On an aggregate level, this could excessively expose democratic processes and the public dialogue to the influence of narrow private interests. Chamath Palihapitiya, a former Facebook executive, even goes so far to say that “the short-term, dopamine-driven feedback loops that we have created are destroying how society works.”[41]

Tech companies struggle to respond. Faced with increasing criticism and pressure from concerned parents and civil rights groups, tech companies have started to address the issue of smartphone overuse, such as Apple through its "Screen Time". At the same time, Apple has been reported to restrict other third-party screen-time and parental-control apps in its App Store.[42]

This could be an indication of how difficult it is for tech companies to adjust their business model. Policymakers have also started to react to the issue. In the US, a "Social Media Addiction Reduction Technology Act" was just recently introduced to congress, which aims to force social media companies "to take measures to mitigate the risks of internet addiction and psychological exploitation".[43]

[38] Axios (2017). Sean Parker unloads on Facebook: “God only knows what it's doing to our children's brains.”
[39] Eyal, Nir. (2019). Hooked: How to build habit-forming products.
[40] Fogg, B.J. (2008). Mass interpersonal persuasion: An early view of a new phenomenon.
[41] Washington Post (December 12, 2017).
[42] New York Times (April 27, 2019).
[43] Hawley, Josh (2019). Social Media Addiction Reduction Technology Act.

Erosion of civil rights through algorithmic bias

Predictive algorithms surround us, whether it is the autoplay function on YouTube, a movie recommendation on Netflix or an advertisement on Google search. Predictive algorithms are frequently deployed for loan decisions, university admissions and recruitment but also for police work, at airports, borders or in judicial decisions. But while these statistical data analysis based tools are assumed to be efficient and free of human prejudice, bias and discrimination can enter their models and outcomes through various ways.

Predictive analytics bears the risk of replicating or even amplifying human bias. For example, when algorithmic recruitment tools use historical application letters, this can lead to a gender bias, as experienced by Amazon. In the same way, algorithms for the risk assessment of US judges to determine bail and sentence limits, based on datasets that reflect historical inequalities such as racial discrimination, can repeat that bias.[44.] In predictive policing, such as the National Data Analytics Solution (NDAS) in the UK, the use of algorithms based on police 'stop and search' data can in the same manner lead to a manifestation of historical ethnical biases in police checks.[45.] A lack of diverse datasets can also lead to bias against minorities, such as the facial recognition systems used at US airports.[46]

'Black box' algorithms. AI systems based on machine learning can also come with so-called 'black box' issues, which means that even the developers cannot inspect easily how an algorithm comes to its results. This creates an additional risk for bias, as potentially discriminating criteria cannot be easily detected.

Data availability and rapid progress in AI systems will see an increased use of predictive analytics, not only by companies, banks and recruiters, but by also government institutions and authorities. If the related shortcomings and risks are not addressed adequately, the technology-based amplification of bias and prejudice, as well as statistical flaws and errors, could lead to an entrenchment of historical inequity. This could undermine protection from discrimination and equal treatment, which is enshrined in the constitutions of modern democratic societies.[47]

Impact of AI and automation on competitiveness and support for democracy

Democracy needs the support of the majority of the population for the political system itself and the informed participation of its citizens and voters. But the approval of a democracy by its citizens presupposes their implicit assumption that it will fulfil their economic needs and aspirations. Equal opportunities and the preservation of the competitiveness and economic prosperity of a democratic society are therefore essential for its political stability and the functioning of its institutions. An increasing income gap and the drifting apart of labour and capital income are already causing growing discontent in many Western industrial societies. These divergences could intensify in the coming years as a result of the increasing automation and use of AI.[48]

Uncertainty regarding the scale and speed of disruption to labour markets makes it ever more important to get prepared for the potential consequences of

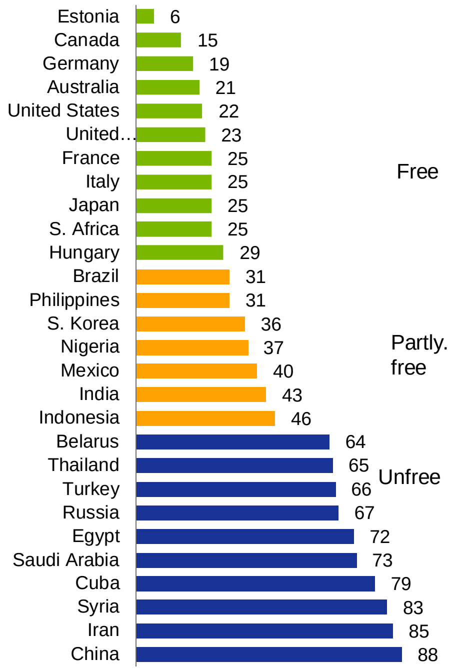
[44] Lee, Nicol Turner et al. (2019) Algorithmic bias detection and mitigation. Brookings.
[45] Guardian (April 20, 2019).
[46] CNET (May 8, 2019).
[47] Council of Europe (2017). Algorithms and human rights.
[48] Heymann, Eric et al. (2018). Digital economics: How AI and robotics are changing or work and our lives. Deutsche Bank Research. EU Monitor.

automation.[49] Otherwise, the stability of consensus-based democratic systems could be seriously undermined. Existential fears and a feeling of irrelevance among a growing portion of the population could increase the leverage of populist, anti-democratic and authoritarian currents that offer supposedly simple solutions in an excessively complex world.[50]

Shift of global competitive advantages. Global competitive conditions are changing rapidly in the age of the data economy. In the past, US tech giants have had a huge lead in this area and could divide the global market among themselves in a flash. While China reacted by sealing off its digital economy and promoting its own tech giants, Europe has already fallen far behind. Hence, the competition for future technological leadership should take place primarily between the US and China, if Europe does not manage to close the gap.

Freedom of internet users, global comparison 11

Freedom on the net index (2018)



Note: index includes obstacles to access, limits on content, violations of user rights

Quelle: Freedom House

Authoritarian and centrally organized societies could increasingly benefit from the seamless adaptation and development of new technologies that are hampered in democratic societies by ethical and legal restrictions, such as artificial intelligence and biotechnology. They also enjoy a level of access to the data of their citizens not compatible with the norms of democratic societies, spurring both AI development and societal control. Their centralised organisation, which was considered a major disadvantage against the technological background of the 20th century, could turn into an advantage in the age of the data economy.[51.] By strengthening their economic success and internal controls, AI could provide authoritarian regimes an advantage over liberal democracies and bolster their position in a renewed competition of political systems for global supremacy. It could also help them counter-prove the apparent lesson of the Cold War that economic success and liberal democracy are immutably intertwined, increasing the attractiveness of the 'authoritarian model' to other countries.[52]

Strengthened by economic and technological success, China is increasingly presenting its system of authoritarian leadership and state capitalism as a superior alternative to Western democracies. If EU members and other democratic countries lose ground in digital and economic innovation, there is a risk that authoritarian structures could become increasingly accepted here as well. This already seems to be the case in some EU countries.[53]

Mass surveillance and strengthening of authoritarianism

Autocratic regimes have been quick to understand both the threats of an uncensored open internet to their political control and stability, and the opportunities that the new technologies offer in state surveillance and control. In fact, the combination of mass data and advanced (AI) technology can give governments unprecedented means to monitor, surveil, control and influence their citizens. Ian Bremmer from Eurasia Group called this the "biggest geopolitical surprise of the last decade", as technology that had originally undermined authoritarian regimes have turned to strengthen them, due to "big data, surveillance and deep learning."[54]

[49] Becker, Sebastian (2019). Digital structural change and the welfare state in the 21st century. Deutsche Bank Research. EU Monitor.

[50] Reid, Jim et al. (2019). Politics, populism and power. Deutsche Bank Research. Konzept.

[51] Council of Europe (2017). Algorithms and human rights.

[52] Wright, Nicholas (2018). How Artificial Intelligence will reshape the global order. Foreign Affairs.

[53] Benner, T. et al. (2018). Authoritarian Advance. GPPi and merics.

[54] Foreign Affairs (February 12, 2019).

Rapid advance in AI-based surveillance technology. Over the last 10 years, the scope of surveillance technologies has reached a new level. It includes all electronic communications, whether email, phone calls, text mail, messenger apps, social media or payments. Search histories, tracking tools and social logins allow the following of users through the virtual space, aggregating their data to individual profiles, which can be psychometrically analysed and categorised through algorithms.

Advances in AI-based surveillance technology, such as facial, voice and motion recognition, together with a web of surveillance cameras in public places, allows the tracking of individuals in the real world. As with progress in other technologies, tools for surveillance together with predictive analytics can both be used to increase security, safety or traffic control, as well as enable governments to control large crowds and predict the formation of protest and riots.

Unprecedented possibilities for government control. For authoritarian states, these tools can help detect and prevent any kind of dissent at an early stage and prevent the formation of opposition and civil right groups that could challenge the concentration of the political and economic power of a ruling elite. As authoritarian governments can enforce access to all information and data collected and stored by private companies (which are often not clearly separated from the government anyway), the state's means of monitoring and control can comprise all aspects of citizens' lives. The internet of things, including all kinds of ‘smart devices’ that apply audio-visual and other sensors within private and public places, could inflate the surveillance grid. Social credit scoring systems are additional powerful tools that encourage self-censorship and preemptive subordination while they allow dissenting citizens to be excluded from social and economic life. Together with censorship and the ring-fencing of the internet as well as the control of information flow through news platforms and social media, these tools allow for what some have called the ‘rise of digital authoritarianism’.[55]

In fact, the ‘dual use’ nature of surveillance technologies makes it often difficult to distinguish between civilian or policing applications on the one hand and political oppression on the other. A surveillance infrastructure for traffic control or for fighting crime could also be used as a tool to monitor or crackdown on the opposition.

China at the forefront of surveillance technology. When it comes to the development and implementation of surveillance technology such as facial recognition, China has become a global front-runner. China's two top funded AI companies are in the fields of surveillance.[56] As part of its 2030 AI strategy, China has rolled out around 200 million surveillance cameras nationwide, according to a CNBC report.[57] In its northwestern autonomous region of Xinjiang, Chinese surveillance firms are tracking the movements of more than two million people, according to Reuters.[58] It was also reported that Chinese police have started to install data extraction software on citizens' smartphones during routine security interactions such as subway security.[59] Almost all of China's 1.4 billion citizens are registered in a facial recognition database.[60] China's plans to introduce a national social credit system by 2020, which is currently being tested in several cities, have raised global attention and concerns. The system assigns scores to citizens according to their behaviour in

[55] Freedom House (2018). Freedom on the net 2018.
[56] CBInsights (February 12, 2019).
[57] CNBC (May 16, 2019).
[58] Reuters (February 17, 2019).
[59] Financial Times (July 4, 2019).
[60] CNBC (May, 2019).

various aspects of their lives and punishes or rewards them accordingly, e.g. by denying them access to transportation, insurance or investment products.[61]

Proliferation of surveillance technology. Chinese companies are also a major exporter of their surveillance technology to other governments and security agencies, partly under the framework of China's Belt and Road Initiative but also beyond that. According to Steven Feldstein from Boise State University, China has provided AI surveillance technology to more than 50 governments, including Malaysia, Singapore and Zimbabwe or Serbia, making the adaptation of surveillance technology a global phenomenon.[62] According to Feldstein, "around the world, AI systems are showing their potential for abetting repressive regimes and upending the relationship between citizens and state, thereby accelerating a global resurgence of authoritarianism." The report considers the export of AI technology to authoritarian regimes a key element of Chinese geopolitics. Feldstein sees technologies such as facial recognition, which are based on massive databases and advanced machine learning technologies, as a "game changer for authoritarian efforts to shape discourse and crush opposition voices".

Different from authoritarian countries, governments in democratic countries are often limited by legislation and public opposition towards the extensive use of surveillance technologies. But also here, governments have an incentive to use these technologies to fight terrorism and crime. Terror attacks and crime incidents can shift public opinion in favour of such applications.[63] The US deployed facial recognition technology at border crossings to Mexico as part of a pilot project and rolled out a facial recognition system to confirm the ‘biometric exit’ of departing passengers at US airports.[64] Other countries such as Germany, the UK and Japan have started to use or test facial recognition technology in public places.[65]

Balance between security and the protection of rights. In countries with strong democratic institutions, the establishment of a broad surveillance infrastructure requires finding a balance between public safety and security on the one hand and the protection of individuals' rights and freedoms on the other. Parliamentary and judiciary control is a prerequisite to preemptively address the risk of abuse through political actors and authorities. Also here, the role of private companies in collecting and analyzing users’ data needs to be scrutinised, both regarding their collaboration with government bodies as well as domestic and external third parties.

Surveillance technologies could become a risk to democracy in vulnerable democratic societies that are already on the way towards more authoritarian structures, as now observed in emerging markets, whether in Asia, Africa or Latin America, as well as in some EU countries. There, governments might increasingly use surveillance technologies to "monitor the activities of political opponents and civil society, and take preemptive action against potential challenges to their authority."[66]

Bans and limits to surveillance. To protect citizens' rights, policymakers in some countries or communities have already moved ahead to prevent the risk of abuse, such as in the US cities of San Francisco, Somerville and Oakland, which ban the use of facial recognition software by the police and other

[61] The Guardian (March 1, 2019).

[62] Feldstein, Steven (2019). China is exporting AI surveillance technology to countries around the world. Newsweek (April 23, 2019) and Reuters (August 2, 2019).

[63] In Germany, a 2018 survey found that 87% of the population is in favor of video surveillance of public places. Only 10% consider this an excessive privacy intrusion (Forsa, 2018).

[64] The Verge (April 18, 2019).

[65] Politico (June 24, 2019), Der Spiegel (October 12, 2018) and Reuters (August 13, 2019).

[66] Feldstein, Steven (2019). The road to digital unfreedom: How Artificial Intelligence is reshaping repression. Journal of Democracy, January 2019.

agencies.[67.] A US court has just ruled that users can sue Facebook for using their facial data for its own facial recognition software without their consent.[68] Europe, which lags behind China and the US in the development of AI, is leading – in data protection – in the setting of ethical standards and regulation with respect to surveillance technology. The Commission's expert group on AI declared in guidelines on the development of "Trustworthy AI" in Europe that "individuals should not be subject to unjustified personal, physical or mental tracking or identification, profiling and nudging through AI powered methods of biometric recognition (...)." The "exceptional use of such technologies, such as for national security purposes, must be evidence based, necessary and proportionate, as well as respectful of fundamental rights."[69]

Urgently needed: A digitally literate society

The digital transformation affects all aspects of people's private and public lives, whether in democracies, flawed democracies or authoritarian states. The speed, lack of precedents, complexity and often the subtle nature of the observed changes pose a formidable challenge to governments and citizens.

Technology is neutral; its application is not. Beyond all the undoubted opportunities and benefits offered by a globally connected world and its rapid technological progress, it needs to be better understood how deeply this can affect the political dialogue and interaction between governments and the electorate. While technology itself is neutral in its use and potential abuse, the policymakers and companies in control of the technology are not.

Technology and democracy remain compatible. In this report, we focus on the risks and challenges that the digital transformation of the last decade pose for democracy. At the same time, we believe that the benefits of the data economy and technological progress in key areas such as AI and automation remain fully compatible with a stable, dynamic and prosperous democratic society based on liberal values and the protection of individual rights and freedom. As over the past century, technology and communication could remain powerful instruments to enable citizens, enrich the societal discourse and strengthen democratic institutions.

For this, democratic societies need to react to the side effects and threats posed by technology to their institutions and their citizens' rights, both at home and from abroad. Governments need to update regulation, competition rules and supervision to account for the transformed requirements of the data economy. Companies need to ensure that their business models and products are compatible with constitutional rights and the integrity of democratic institutions and processes. Users and citizens need to better understand the algorithms and designs behind their apps and devices as well as the mechanics of the data economy. Democratic societies need an informed dialogue on data and technology ownership on how to share the fruits of technological progress and on how to prevent increasing asymmetries in wealth and power from destabilizing their foundations.

EU has become a role model for AI and data regulation. The EU and its member countries lack big tech players and struggle to catch up in the global race for AI dominance, seemingly mainly between the US and China. However, it appears that in Europe the challenges posed by technology to democratic societies have een addressed better than elsewhere.[70] Over recent years, the EU have taken a

[67] New York Times (May 14, 2019) and Vox (July 18, 2019).
[68] Reuters (August 8, 2019).
[69] European Commission (June 26, 2019).
[70] European Parliament (2019). EU policies – delivering for citizens: Digital transformation.

front seat in respective regulation and initiatives, whether it is the protection of privacy and user rights (GDPR), its plan against disinformation or its AI Alliance, a multi-stakeholder forum aimed not only at fostering AI investment and research, but also at answering pressing ethical and legal questions. It is a learning process: shortcomings and loopholes will need to be addressed, and rules and regulations adjusted in order to balance economic, societal and political aspects. But the EU's message is clear: technological advance and the data economy belong to all citizens.

Kevin Körner (+49 69 910-31718, kevin.koerner@db.com)

The above information does not constitute the provision of investment, legal or tax advice. Any views expressed reflect the current views of the author, which do not necessarily correspond to the opinions of Deutsche Bank AG or its affiliates. Opinions expressed may change without notice. Opinions expressed may differ from views set out in other documents, including research, published by Deutsche Bank. The above information is provided for informational purposes only and without any obligation, whether contractual or otherwise. No warranty or representation is made as to the correctness, completeness and accuracy of the information given or the assessments made.

In Germany this information is approved and/or communicated by Deutsche Bank AG Frankfurt, licensed to carry on banking business and to provide financial services under the supervision of the European Central Bank (ECB) and the German Federal Financial Supervisory Authority (BaFin). In the United Kingdom this information is approved and/or communicated by Deutsche Bank AG, London Branch, a member of the London Stock Exchange, authorized by UK's Prudential Regulation Authority (PRA) and subject to limited regulation by the UK's Financial Conduct Authority (FCA) (under number 150018) and by the PRA. This information is distributed in Hong Kong by Deutsche Bank AG, Hong Kong Branch, in Korea by Deutsche Securities Korea Co. and in Singapore by Deutsche Bank AG, Singapore Branch. In Japan this information is approved and/or distributed by Deutsche Securities Inc. In Australia, retail clients should obtain a copy of a Product Disclosure Statement (PDS) relating to any financial product referred to in this report and consider the PDS before making any decision about whether to acquire the product.

Printed by: HST Offsetdruck Schadt & Tetzlaff GbR, Dieburg

ISSN (Print) 1612-0272 / ISSN (Online): 1612-0280