KKI

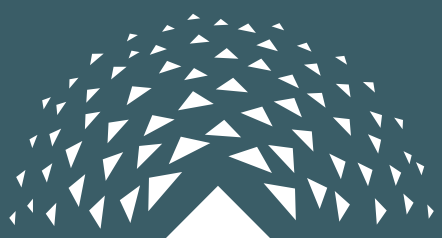
Policy Brief

E-2020/60

Will COVID-19 Prompt Global Ethical AI Standardization?

Covid-19 lehetséges hatása a mesterséges intelligencia globális etikai szabályozására

ANNA JUHOS



INSTITUTE FOR FOREIGN AFFAIRS AND TRADE

KKI Policy Brief
Series of the Institute for Foreign Affairs and Trade

Publisher:
Institute for Foreign Affairs and Trade

Reviewer:
Tamás Baranyi

Typesetting:
Tamás Lévárt

Editorial office:
H-1016 Budapest, Bérc utca 13-15.
Tel.: + 36 1 279-5700
E-mail: info@ifat.hu
http://kki.hu

ISSN 2416-0148

Abstract: The use of high-tech has undeniably become the latest measure of relevance in the international community. The COVID-19 crisis has prompted many countries to experiment with Artificial Intelligence (AI) systems more widely in order to bring the situation under control. As the main trendsetters for tech regulation and experimentation, the EU, the US, and China have shown us examples of both best practices and less successful scenarios, raising important questions in terms of the ethical use of the latest technologies, data privacy, and fundamental rights. In an endeavor to assess the current state of affairs and ethical use in the digital realm, this analysis raises awareness of both government practices and discrepancies between private and public sector approaches. Given the tremendous opportunities AI can provide for all societies, this analysis calls for a more active role of the international community by setting the red lines and developing a clear and detailed ethical regulatory and sanctioning framework.

Keywords: data privacy, EU, China, US, artificial intelligence, surveillance, ethics

Összefoglaló: *A nemzetközi közösségben egyértelműen az új technológiák használata vált a relevancia legújabb meghatározójává. A COVID-19 válsághelyzet számos országot arra ösztönzött, hogy felgyorsítsák és kiszélesítsék mesterséges intelligencia (AI) rendszereik használatát. Az új technológiák szabályozásában és az azokkal való kísérletezésben élenjáró entitások, az EU, az USA és Kína fontos példával szolgálnak az AI-rendszerek használatának előnyeire és árnyoldalára nézve is. Mindez számos kérdést vet fel a legújabb technológiák etikus használatát, valamint az alapvető jogok és az adatbiztonság védelmét illetően. Jelen elemzés célja, hogy a három esettanulmányon keresztül bemutassa az országok közötti és az országokon belüli, kormányzati-vállalati eltéréseket, ellentmondásokat, a szabályozó környezetet és annak hiányosságait. A példák rámutatnak, hogy az AI-rendszerekben rejlő példátlan lehetőségek csak akkor hozhatnak pozitív előnyöket a társadalmak számára, ha egyértelművé tesszük a korlátokat, a szankciós és felelősségrevonási rendszert, valamint az etikus technológia-használat kereteit, amelynek érdekében a nemzetközi közösség részéről egy sokkal proaktívabb fellépés szükséges.*

Kulcsszavak: *adatvédelem, EU, Kína, USA, mesterséges intelligencia, megfigyelés, etika*

Introduction

The global COVID-19 crisis has prompted many governments to speed up their country's digital transformation and put more emphasis on tech-related skills, solutions, and infrastructure. In order to achieve quick results, contain the spread, and develop vaccines, to also prove their leadership's aptitude both domestically and in the international community, countries have resorted to different methods and policies.

The EU, the US, and China have long been the main trendsetters in digital competitiveness. They have been chosen as case studies for this analysis due to their role in shaping the global discourse on digitization and privacy rights. As highlighted by their different approaches to tackling the COVID-19 pandemic, their examples provide important insights into the general concerns and practices that have an impact on the development of tech regulation.

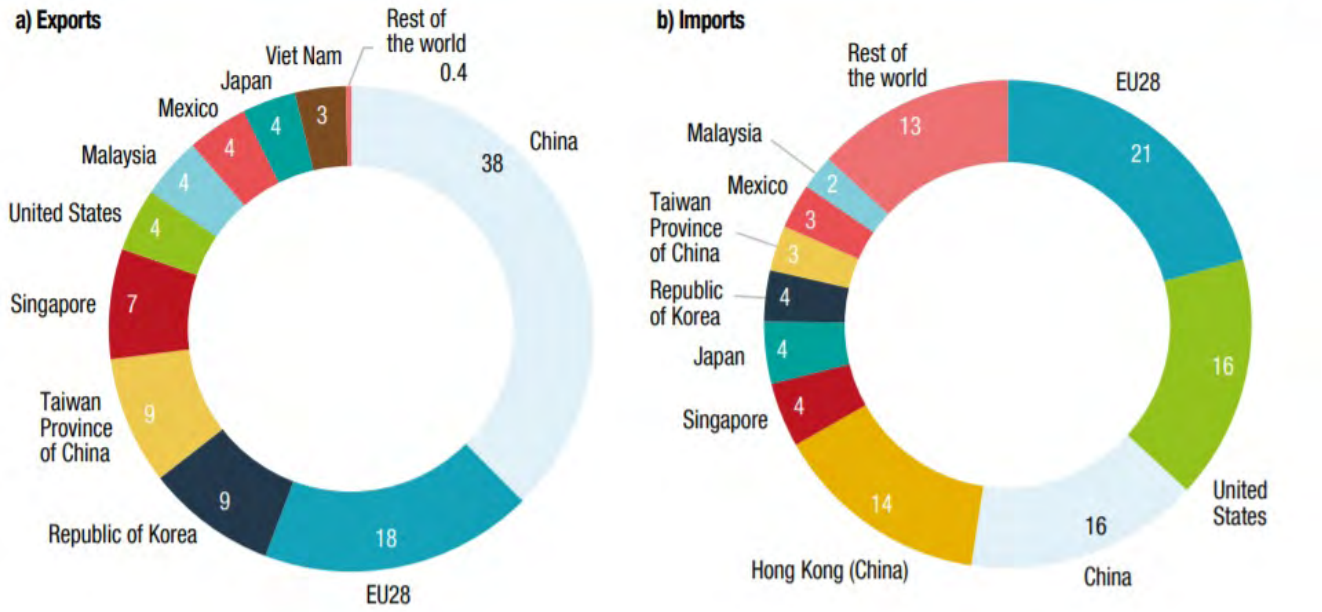
As part of the current, crisis-induced tech surge, "*AI [Artificial Intelligence] is being used to fight the [corona]virus on all fronts, from screening and diagnosis to containment and drug development*." Numerous articles highlight this claim to reassure citizens that their governments are on the right track to effectively handling the crisis. Utilizing the latest technologies, however, has exacerbated significant political-ideological disparities and raised awareness of the fact that more ethical tech regulation is required.

This analysis evaluates the different responses and regulatory approaches by the three most important players in the field. Furthermore, it provides recommendations and examples for transparent, fair, and regulated AI use, where data privacy and civil liberties are accounted for. For the evaluation of the ethical AI technology usage by the EU, the US, and China, the analysis takes the UN recommendations and OECD principles as its baseline. Thus, it argues that AI systems should benefit the people, ensure a fair and just society (rule of law, human rights, and democratic values), work in a secure and safe way, be transparent, and the organizations and individuals developing, deploying, or operating AI systems should be accountable.

The Digital State of Play

To substantiate the chosen case studies, first we have to take a look at the digital state of play. The 2019 Digital Economy Report of the United Nations Conference on Trade and Development (UNCTAD) and the charts below show a clear divide, with a handful of players (mostly the EU, the US, and China) taking the lead and controlling the trade in information and communications technology (ICT) goods exports and imports, leaving a share of 0.4%, and 13% to the rest of the world, respectively.

Figure 1
Geographical distribution of trade in ICT goods, 2017 (Per cent)



Source: UNCTADStat

The Report claims that *"The economic geography of the digital economy does not display a traditional North-South divide. It is consistently being led by one developed and one developing country: the United States and China."* Furthermore, these two countries account for 50% of global spending, 75% of blockchain technologies, 50% of global spending on the Internet of Things, and 90% for the market capitalization value of the world's 70 largest digital platforms. The seven "super platforms" (Microsoft, Apple, Amazon, Google, Facebook, Tencent, Alibaba) account for two thirds of the total market value. Europe's share is a mere 4%, while Latin America or Africa is around 1%.

When it comes to regulation, the International Telecommunication Union's (ITU) ICT regulatory tracker also confirms the above trend. Tracking 193 countries over 12 years (2007–2018), and using first-hand information from ICT regulators and ministries, the tracker displays the region-specific number of top countries contributing to ICT regulatory developments. The Tracker measures 50 indicators along four clusters, namely: the functioning of the regulatory authority; the mandates – who regulates what; the regime – what kind of regulation exist; and the competition framework for the ICT sector.

Out of the top 25 countries, 20 are from Europe, one from the Asia-Pacific, and one from the Americas, leaving none from Africa or from the Commonwealth of Independent States (CIS). Therefore, while we talk about digital competitiveness, ethical use of technologies, and debates in the WTO or the ITU about different regulatory frameworks for internet and data usage,

it is important to note that a considerable number of countries and regions do not experience quick digital transformations, and they are left out of significantly shaping the discourse.

Table 1
Top ICT Regulators by Region

Region	Countries in World top 25
Africa	0
Americas	3
Arab	1
Asia-Pacific	1
CIS	0
Europe	20

Source: ICT Regulatory Tracker 2017.

When it comes to tech regulation, with nearly half of all proposals coming from Europe, it is way ahead in this race by being the global trendsetter. This goes against the argument of some experts who argue that the EU has a structural problem, it is burdened by overregulation and a lack of venture capital and investments. According to these critics, as a result of its rigid regulatory approach, for the EU to be a tech leader is not a question of 'when', but rather of 'how'. The above trends refute these claims.

On the other hand, as the charts above also show, the questions of 'when' and 'how' are still important questions for most countries. It is important to highlight that we are still witnessing different phases of digitization all over the world. The vast majority of countries and territories are still developing their first (introduction and adoption) or second wave of digitization (diffusion of the internet and its platforms), while some, like the EU, the US, or China are already experimenting with the third wave (robotics, big data, AI, IoT). Questions about ethical digital regulations and privacy rights are therefore considerably shaped by these three entities, with the EU, the US, and China as the most influential and active players in the digital sphere. These entities' diverse policies provide important precedents and guidelines for all other countries entering the digital race. Therefore, a thorough assessment of their policies and best practices for digitization and privacy rights is needed. This could help establish the practice of ethical and trustworthy technology usage as the baseline. Moreover, it could help develop a clear framework with rules, monitoring, and sanctioning for the countries that are about to join the third wave of digitization and are looking for guidance.

How to use High-tech Responsibly? does it have to be a Privacy Rights vs. Public Security Trade-off?

One of the most important tech questions has been how to handle what the World Health Organization (WHO) has described as an 'infodemic". The report says that *"the 2019-nCoV outbreak and response has been accompanied by a massive (…) over-abundance of information – some accurate and some not – that makes it hard for people to find trustworthy sources and reliable guidance when they need it."* Simultaneously, more and more news outlets report about the growing number of cyberattacks, malign activities, and foreign adversarial disinformation especially by Chinese, Russian, and Iranian actors, intended to undermine security and expose vulnerabilities in the EU and the USA. This shows the frictions between China, the EU, and the US when it comes to ethical technology use and regulations. However, this goes well beyond the different categorizations describing these actors as the regulatory-cautious EU, the tech giant-lobbied US, or the centrally controlled China.

For the assessment of their approach, it is worth recalling the remarks of Henry Kissinger in his 2018 article "How the Enlightenment ends". He argues that *"Truth becomes relative. Information threatens to overwhelm wisdom. (…) The digital world's emphasis on speed inhibits reflection; its incentive empowers the radical over the thoughtful; its values are shaped by subgroup consensus, not by introspection. (…) Artificial Intelligence will in time bring extraordinary benefits to medical science, clean-energy provision, environmental issues, and many other areas. But precisely because AI makes judgments regarding an evolving, as-yet-undetermined future, uncertainty and ambiguity are inherent in its results. (…) And governance, insofar as it deals with the subject, is more likely to investigate AI's applications for security and intelligence than to explore the transformation of the human condition that it has begun to produce."*

The evaluation of the EU, China, and the US raises important questions for the rules of the game, i.e. data regulation and privacy. While some argue that the use of AI technology is in line with public safekeeping, it is a crucial question under what circumstances health authorities' access to phone GPS and credit card data might seem too much of a prioritization of strong state measures over individual liberties and privacy. The question arises who defines what the ethical use of technology in a certain country entails and what the red lines are. Additionally, what is the right balance between maintaining liberties, not curbing privacy rights, but at the same time utilizing technological advantage to provide for better public security and safety? Will strict and quick digitization initiatives pushed through by governments also be considered more effective? These questions all call for a much more regulated digital space globally, with these most technologically competitive countries as the real shapers and trendsetters. This necessitates a closer evaluation of their practices and policies.

The Good, the Bad, and the Ugly

The Good

The EU's case represents a relatively cautious and rather strict but advanced regulatory approach. It focuses both on competitiveness and fairness, which makes it the best example among the three case studies. The EU's 2019 Ethics Guidelines for Trustworthy Artificial Intelligence clearly define that a trustworthy AI should be *"lawful - respecting all applicable laws and regulations; ethical - respecting ethical principles and values; and robust - both from a technical perspective while taking into account its social environment."*

With an already functioning prohibitive approach, the General Data Privacy Regulation (GDPR), the European Strategy for Data, and the White Paper on Artificial Intelligence, Europeans can in general argue that they are better off when it comes to their privacy and data protection. The new EU Commission's strive to enhance development and competitiveness through digitization, and their commitment to safe and ethical standards have introduced new debates among policymakers and academics.

In terms of competitiveness, the EU still needs to catch up with its competitors. The aim of the Europe 2020 Strategy to reach 3% of EU GDP for Research, Development and Innovation (R&D&I) is a significant step forward. In terms of R&D&I intensity (i.e. expenditure as a percentage of GDP), the EU is more or less on par with that of China. However, mainly because of lower levels of private investments, in terms of R&D&I spending the EU is still lagging behind the US.

In terms of fairness, even though the COVID-19 crisis has refocused most energies to health care, the internal market, and jobs, both European Commissioner for Competition Margrethe Vestager and Commissioner for Internal Market and Services Thierry Breton have made clear their commitment to fundamental rights and applying technically robust, accurate, and trustworthy AI systems. The GDPR makes explicit consent a condition in relation to high-risk AI, and the White Paper on AI also specifically highlights that *"the gathering and use of biometric data for remote identification purposes, for instance through deployment of facial recognition in public places, carries specific risks for fundamental rights. (…) In accordance with the current EU data protection rules and the Charter of Fundamental Rights, AI can only be used for remote biometric identification purposes where such use is duly justified, proportionate and subject to adequate safeguards. In order to address possible societal concerns relating to the use of AI for such purposes in public places, and to avoid fragmentation in the internal market, the Commission will launch a broad European debate on the specific circumstances, if any, which might justify such use, and on common safeguards."*

Such actions and clarifying guidelines are good means for increasing trust in the governments and also to enhance trust in the wider application of AI systems among European citizens. With its slower and more regulatory approach

compared to the two competing giants, the EU framework mainly builds on trust, encourages trustworthy AI certification even in low-risk sectors, and sets out a clear timeline for tech rollout. The EU has even explicitly argued against the creation of new forms of automated social control through AI systems and advocated for the least liberty-infringing alternatives. In response to ideas about a voluntary COVID-19 tracking app by the Pan-European Privacy Preserving Proximity Tracing (PEPP-PT) project, among others Germany's Global Ethical AI Consortium has made it clear that such technology use is an option only if it complies with strict EU privacy and ethical rule.

The EU is often accused of overregulation and bureaucracy. However, with the GDPR the EU has set the standards which could serve as a basis for international regulation for privacy and data protection. Similarly, its ethical AI principles could also have a globally positive effect. Its focus on ethically justifiable, necessary, and proportionate action, the use of AI technologies for optimized clinical assessments, drug testing, and research have all maintained the EU's role as an ethical standards setter. This, however, sets a different example compared to China or the US. Eleonore Pauwels, Director of the AI Lab at the Woodrow Wilson Center has even described China as a "digital dictatorship" and the US system as "surveillance capitalism". Compared to the EU, the rules of the game in these countries show a much more mixed, more specifically, a bad, and ugly picture.

The Bad

While the discourse in the EU centres mostly on privacy and ethical use, one of the early responses at the epicentre of the pandemic was increased surveillance, along with questionable data collection practices. Considering that eight out of the top ten most-surveilled cities are located in China, the Chinese Communist Party's (CCP) increased surveillance methods – coupled with tightened control, disenfranchisement, and loss of privacy – came as no surprise. As a comparison, the city of Chongqing with its 2,579,890 cameras for 15,354,067 people (168.03 cameras/1,000 people, or 1 camera/5.9 people) already dwarfed the 68.40 cameras/1,000 people in London, the 11.18 cameras/1,000 people in Berlin, or the 5.61 cameras/1,000 people ratio in Washington DC in 2019.

Dirks and Cook, Yang and Zhu, Mozur and Krolik, among others, argue that the pandemic has considerably contributed to the expansion of the 21st-century Chinese police state in terms of its scope and methods, enabling the widespread use of face-recognition cameras, geolocation data collection, and internet censorship. In the Chinese case, concerns have been raised a while ago that companies like Alibaba or Tencent transmit their customers' data to authorities. The CCP's response to COVID-19 has not only raised questions about the disenfranchisement of citizens, the possible extension of strict measures even after the pandemic, but it has also led to increasing

concerns about a potentially more widespread crackdown on minorities and persons deemed a "national security risk". There is growing fear of the impact of automation and digitization, and how these will exacerbate the repressive state practices which have been going on for a while. The transition from "over the skin" to "under-the-skin" surveillance with body temperature-measuring AI systems, or DNA phenotyping and facial mapping, a practice already used in the case of the Uyghur minorities, have propelled many to ring the alarm bells and even boosted dystopian fantasies about algorithm-controlled, ranking-system categorized citizens, such as in Marc-Uwe Kling's Qualityland.

Set in the framework of ethical and trustworthy AI use, the Chinese case shows that – with disenfranchisement and disregard for human rights, lack of transparency and accountability – it does not comply with any of the recommendations and principles which aim at ensuring a fair and just society.

This is in sharp contrast when it comes to measures in the wider region. Singapore and South Korea have both responded to the pandemic and 'infodemic' with the same method – increased surveillance –, but they have also used their authority to empower citizens through confidence-building measures and by sharing all available information to counter fake news and to increase social trust in the government. As Lee Tae-ho, South Korean vice minister of foreign affairs argued, "public trust has resulted in a very high level of civic awareness and voluntary cooperation that strengthens our collective effort." This approach resembles the EU's trust-building narrative.

One could argue that the question of empowerment or disenfranchisement even in the digital realm all comes down to the ideological, and cultural differences, and eventually the type of regime. If we legitimize such a claim, the hope for worldwide, uniform, ethical digital regulations has already come to a dead end. At the moment, the rather anarchical digital world's only recourse against malign actors in the cyberspace seems to be attribution and arbitrary sanctions. However, the problem is more complex than dividing the world into law-abiding democratic, and malign authoritarian entities. It is not only a question of regulation coming from the top, from governments, or supranational entities. It also raises awareness of intra-country, bottom-up dynamics and impulses, thus actions coming mostly from the private sector, not necessarily completely in line with government guidelines. Overall, it creates a problem where – against governments or supranational entities – companies and interest groups with high stakes and influence create the rules of the game.

The Ugly

Compared to the two cases above, the US case shows a rather mixed picture. Regarding the COVID-19 crisis, timing and quick government action might have been everything, as accusations against the US leaders' slow decisions claim. The idea of a national coronavirus surveillance

system to allow federal government access to patients' data and real-time hospital needs in all US states has been floated, but it was almost immediately officially denied by the White House. However, at the same time, Apple and Google have rolled out a new contract-tracking app, which uses Bluetooth technology to alert people in case they have been near people infected with COVID-19. The companies say that all procedures are transparent and observe privacy rights. In terms of regulatory frameworks, from the governments' side there have been various sets of AI ethical principles and standards published by the White House, the Department of Defense, the National Security Commission on Artificial Intelligence, or the National Institute of Standards and Technology, some even already under the Obama administration. Most of them build on the same principles of transparency, consent, and consequences, although mainly without clear sanctioning or monitoring guidelines. On the tech firms' side, many companies have set up different toolkits, such as the 'AI Fairness 360' by IBM, Facebook's 'Fairness Flow', or Google's 'What-If Tool' to check unwanted bias in data sets and machine learning models.

However, in the case of many tech firms, the argument goes that they only pay lip service to ethical standards, and in reality, they have lobbied hard not to allow stronger data regulation. Over the past couple of years there have been several controversies which support the claim about non-compliance: "Facebook's breach of private data on more than 50 million users to a political marketing firm hired by Donald Trump's presidential campaign, revealed in March 2018; Google's contract with the Pentagon for computer vision software to be used in combat zones, revealed that same month; Amazon's sale of facial recognition technology to police departments, revealed in May; Microsoft's contract with the U.S. Immigration and Customs Enforcement revealed in June; and IBM's collaboration with the New York Police Department for facial recognition and racial classification in video surveillance footage, revealed in September."

The problem is that in these cases the line between AI systems used for public or private benefit is rather blurry. And while there have been important guidelines at the federal level, depending on the geographical distribution and lobby power of tech giants, detailed regulation has not come from Washington DC but from the states. In this framework, the options for no regulation, voluntary commitments, or moderate regulation to adjust technologies to account for algorithmic bias or discrimination have been companies' favoured choices. By creating restrictive legal frameworks for controversial technologies, some states (Arizona, California, Florida, Idaho, Illinois, Massachusetts, Nevada, New Jersey, New York, and Washington), however, have taken a harder stance.

In this scenario, many raise awareness of the problem of ethics-washing, i.e. the rather empty promises to tackle system bias without real action, as in the case of many big companies and their powerless ethics boards. While the US framework does not yet come close to an EU-wide GDPR regulation, compared to China, it still leaves much bigger room for action by citizens to raise their voice and express their objection. For example, in 2019, as a result

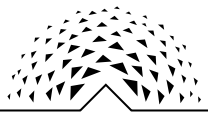
of public initiatives, San Francisco, Oakland, (California), and Somerville (Massachusetts) banned the public use of face recognition, while at the same time Microsoft and Google employees have also become more vocal against their companies' use of AI for surveillance and for tracking migrants.

While there is a plan to develop a data ethics framework by December 2020 in order to help US agencies "systematically identify and assess the potential benefits and risks associated with the data they acquire, manage, and use", there is much more the federal government can and should do. So far it seems federal regulations have been more preoccupied with economic and competitiveness considerations than with AI ethics. In this regard, President Trump's recent executive order affecting Section 230 and companies' liability is understood by many not as a regulatory initiative, but rather as a personal revenge, a curtailment of free speech and an accusation of these companies for political activism and bias. Set against our baseline principles, the US case shows a mixed picture with the ugly instances of ethics-washing, arbitrarily regulated surveillance by tech giants, and questionable guidance and regulatory policies by the government.

The Rules of the Game

As the above examples show us, opportunities provided by AI to improve our lives are enormous, but we should not fall for light-hearted promises and solutions. Paul Nemitz, Principal Advisor in the Directorate-General for Justice and Consumers of the European Commission, one of the architects of the EU's GDPR argues that "not regulating these all pervasive and often decisive technologies by law would effectively amount to the end of democracy."

As for the 'infodemic' and malign activities, the vast majority of the citizens and companies still need to get better acquainted with the measures to effectively recognize and counter cyberattacks and to focus not only on prevention but also on resilience. We have seen positive examples of citizen empowerment and how clarifications and public discourse can all build trust both in governments and their preventive, beneficial, and trustworthy use of AI systems. This trust is also reflected in the Reuters Institute Digital News Report 2019, according to which concern about misinformation and disinformation is high in the US (67%) but much lower in Austria (40%), Norway, Switzerland (39%), Germany (38%), and the Netherlands (31%). (For China, data was not available for this measure.) When it comes to concerns about misuse of personal data, the percentage of internet users aged 16 to 64 who say they are worried about how companies use their personal data is 66% in the US, 62% in China (65% in Hong Kong), 54% in Germany, 50% in the Netherlands and Austria, and 47% in Sweden. All governments should therefore realize that dialogue, awareness-raising, trust,



and empowerment of their citizens is of utmost importance in their legitimization of AI usage, any sort of data collection, as well as for resilience. While there are numerous guidelines and position papers written in the EU and the US, there are also some promising, frameworks developing internationally. These are the United Nations Interregional Crime and Justice Research Institute's Centre for Artificial Intelligence and Robotics in the Hague, or the OECD AI recommendations, signed by 36 members and 8 non-members (Argentina, Brazil, Columbia, Costa Rica, Malta, Peru, Romania, Ukraine). However, before we end up piling up on position papers and strategies, it is important to see that without strict regulations, monitoring, supervision, and sanctioning in the international system we have only come half way.

Therefore, based on the best practices and precedents of the three case studies, in order to guarantee ethical, responsible, and trustworthy AI use both in times of crises and prosperity, the following recommendations are suggested. First, regarding government-to-citizens relations: governments should be transparent, proportional, and just in their data collection and high-tech use. As collectors of huge data sets, they should ensure that citizens have trust in their data use and AI systems. This will enhance citizens' use of these technologies and thus contribute to more widespread digital skills, as well as the country's overall digital competitiveness. Second, in public-private sector relations: digital regulations should explicitly mention under the scrutiny of which independent supervisory body, under what circumstances, if any, and for which purpose private companies could be required to assist and hand over massive data collections to government authorities. Third, in government-to-government relations: through an international watchdog it has to be made clear that opting out results in collective action by the international community against the malign actor. Overall, these should impede government overreach and guarantee that there is no trade-off between public security, individual liberties, and privacy rights.

Conclusion

The different Chinese, American, and European policies and their use of AI systems have set precedents and raised serious questions about accountability, transparency, as well as threats to privacy.

Overall, this analysis calls for much more regulatory, monitoring, and sanctioning action by governments and the international community. Governments should not only act as owners of massive amounts of data but also as regulators of the corporate world, which is quite often seen as setting its own rules of the game. Of course, the lines separating private and public data collection seem mostly blurred in the outlier Chinese case. But malign activities should not stop the regulatory process, and the international community should

expect governments to serve as ethical standard-setters, be at the forefront of this process to ensure the safety and security of their citizens, and build on the positive benefits and opportunities provided by technology.

Governments as well as digitally conscious citizens can make sure that data is handled in a fair, private, and transparent way, intrusive technologies are no longer used, and for example ethical algorithm design (auditing for unwanted biases and discrimination in the algorithms), or differential privacy methods (adding noise/randomness to data to obscure individual identities but not distorting the statistics) are built into the system.

Based on the examples of the analysis, one might ask whether future prospects are a world divided into US, China, and EU regulatory frameworks and datasets. Since many countries which will transition to the third wave of digitization and start applying AI, robotics, and IoT will look for these global trendsetters for guidance, it is of utmost importance to clarify the regulatory framework, with clear sanctioning rules and red lines. Crises and pandemics like COVID-19 call on the international community for more concerted action and thus will propel global ethical AI standardization. Countries which can share best practices should proactively participate and contribute to shaping the global dialogue and help find common ground for actors with currently distinct interests. Only this can disrupt the development of different, arbitrary regulatory environments and a messy future of data regulation causing obstacles for citizens, governments, and economies alike.