

# Challenges of Fourth Industrial Revolution on Ethics in the Public Sector

Maria Bordas

University of Public Service Ludovika, Budapest, Hungary

The Fourth Industrial Revolution represents a fundamental change in the way we live, work, and relate to one another. It is a new chapter in human development, enabled by extraordinary technology advances commensurate with those of the first, second, and third industrial revolutions. The Fourth Industrial Revolution, 4IR, or Industry 4.0, conceptualizes rapid change to technology, industries, and societal patterns and processes in the 21st century due to increasing interconnectivity and smart automation. Moreover, the new IT technology such Artificial Intelligence, Virtual Reality, and wide usage of internet (leading elements of so-called “Fourth Industrial Revolution”), increased efficiency and effectiveness in service delivery in the field of public sector and public administration. Social media have changed and are changing the world, and more importantly, will influence in the future too. The Fourth Industrial Revolution is about more than just technology-driven change; it is an opportunity to help everyone, including leaders, policy-makers, and people from all income groups and nations, to harness converging technologies in order to create an inclusive, human-centered future. The real opportunity is to look beyond technology and find ways to give the greatest number of people the ability to positively impact their families, organizations, and communities. However, the Fourth Industrial Revolution largely presents numerous challenges to public administration in developing countries that lack enough human and material resources to execute the ensuing huge technological advancements. We have acknowledged that the 4IR has different challenges such economic, social, political, and organizational. The fast and major technological changes offer the chance to improve human life, but they also create concerns about the future. One of the biggest fears related to the new technologies is that the robots and the artificial intelligence will replace the human factor in work leading to the “technological unemployment” even the field of public administration. This research is trying to analyze and give some answer to above mentioned issues.

*Keywords:* Fourth Industrial revolution, social media, public administration

## Introduction

This paper aims to shed light on the unethical issues in public administration which emerged due to the Fourth Industrial Revolution (4IR) during the last decades.

Four forms of industrial revolutions evolved during the last two centuries: The first one introduced the steam engine, the second one the mass industrialization, the third one had been known as the digital revolution, and the fourth one had been the 4IR. In the focus of 4IR, we can find the Internet of Things (IoT). Relevance of

---

Maria Bordas, full university professor, Faculty of Public Governance and International Studies, University of Public Service Ludovika, Budapest, Hungary.



the IoT is that during the last decades Internet that became a network and is used every day in a growing manner is sufficiently influencing the life of citizens, e.g., smart cities, robotics, Virtual Reality (VR), and Artificial Intelligence (AI). These fields of the IoT mean the 4IR.

At the beginning of the second millennium, information, and communication technologies, such as smartphones, e.g., dramatically changed the world. Facebook, Twitter, and other social media networks as a new type of media and smartphone technology have changed interpersonal interaction, communication patterns, and social and political discussions. The academics of political science, sociology, international relation, media, and communication have conducted hundreds of studies on various aspects of social media usage (Golan, Arceneaux, & Soule, 2019).

It is well beyond dispute the fact that the Internet is playing an unavoidable role in providing information to the public on homeland political events and the international political arena.

Moreover, the Internet is attracting net users into political life and encouraging them to get involved in political activities.

4IR has had an impact on the economy and society by reshaping all industries, such as production, consumption, transportation, and delivery of services. Citizens can have access to more efficient public services by using e-Government, e.g., in the form of smart cities, that can reach to less consumption of energy and water supply in their home, or electronic case management, when citizens can arrange their administrative cases from home, can get health care services and education on lower prices and on better quality, promote transparency and accountability in the field of state contract and public procurement, and improve communication between citizens and government, etc.

In the developed countries the governments have made effort to give a better life for citizens by using 4IR, which, however, has had certain challenges, as well. One of them is unethical issues in the public sector.

The Internet has become vital for political discussions and political participation. In the beginning, the Internet was used as a one-way communication tool for political parties to inform the public through their websites. In developing countries, especially in Africa, access to the Internet is supported by satellite technology which can overbridge the weaknesses of infrastructure on the field. As a side effect of the pandemic COVID-19, millions of people using the Internet have put pressure on broadband networks.

This paper will examine first, how the 4IR helps the development of ethics in the public sector, in the field of politics, public governance, and public administration, e.g., management of election campaign, better communication with the voters, more efficient public services, administrative case management, transparency, counter-terrorism, etc.

In the second part of this paper the forms of unethical behaviour in the public sector, because of 4IR, will be explored, e.g., using the Internet by the governments to hinder citizens for political goals, intervening in internal matters of other countries for political aims, manipulating voters during election campaigns, using personal sensitive data to attack political enemies, growing state-corruption, etc.

### **Development of the Forth Industrial Revolution (4IR)**

The Fourth Industrial Revolution is growing out of the third but is considered as a new era rather than a continuation because of the explosiveness of its development and the disruptiveness of its technologies. The Fourth Industrial Revolution is the current and developing environment in which disruptive technologies and



trends such as the Internet of Things (IoT), robotics, Virtual Reality (VR), and Artificial Intelligence (AI) are changing the way modern people live and work.<sup>1</sup>

In this case, disruptiveness means that the disruptive technology is one that displaces an established technology and shakes up the industry or a ground-breaking. The Internet of Things, or IoT, is a system of interrelated computing devices, mechanical and digital machines.

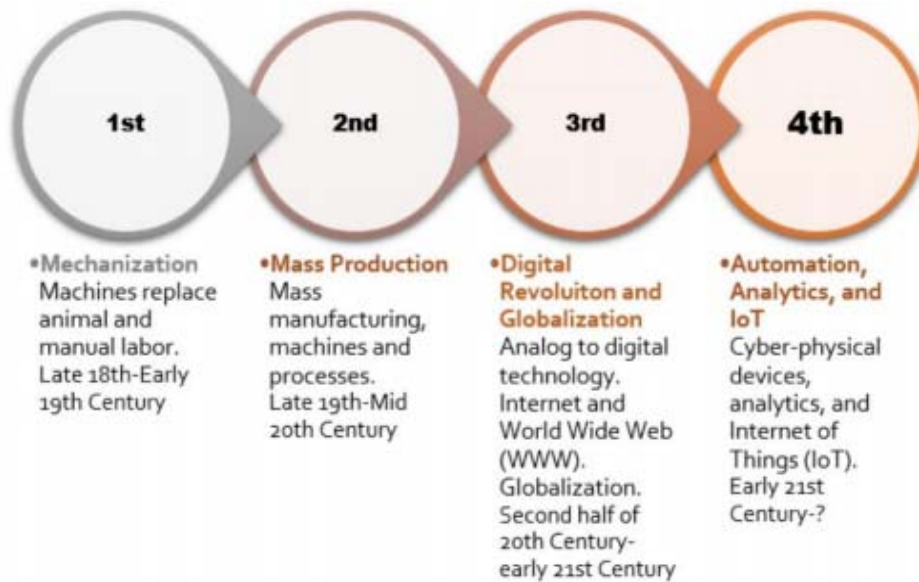


Figure 1. Industrial revolutions (Shank, 2016).

The Fourth Industrial Revolution represents a fundamental change in the way we are living, job, and relate to one another. It is a new chapter in human development, enabled by extraordinary technological advances commensurate with those of the first, second, and third industrial revolutions.

These advances are merging the physical, digital, and biological technology in ways that create both huge promises but at the same time potential insecurity and menace.

Specific technologies of the Fourth Industrial Revolution include, but are not limited to:

- artificial intelligence;
- Internet of Things;
- robotics;
- Virtual Reality;
- mobile devices;
- 3D printing;
- smart sensors;
- big data/analytics;
- augmented reality (AR);

<sup>1</sup> First used the expression of Forth Industrial Revolution by Klaus Martin Schwab (German engineer and economist best known as the founder and executive chairman of the World Economic Forum) in 2016. He determined the Forth Industrial Revolution as “The Forth Industrial Revolution is the ongoing automation of traditional manufacturing and industrial practices, using modern smart technology. Large-scale machine-to-machine communication (M2M) and the internet of things (IoT) are integrated for increased automation, improved communication and self-monitoring, and production of smart machines that can analyze and diagnose issues without the need for human intervention”.



- data visualization;
- cognitive computing;
- location detection;
- customer profiling;
- blockchain;
- quantum computing;
- cloud computing.

The Fourth Industrial Revolution is about more than just technology-driven change. It is also an opportunity to help everyone, including leaders, stock-holders, and ordinary people from all income groups and nations to harness converging technologies to create an inclusive, human-focused future. The real opportunity is to look beyond technology and find ways to give the greatest number of people the ability to positively impact their families, different business organizations, public administrative elements, and communities.

In the developed countries the governments have made effort to give a better life for the citizens by using 4IR, e.g., the IoT, smart cities, administrative case management based on e-Government, more efficient public services, such as energy and water supply, education, healthcare, etc. The 4IR has led to a more democratic government with strengthening transparency, accountability, and better communication with the citizens.

Of this total, 92.6 percent (4.32 billion) accessed the Internet via mobile devices and 4.1 billion are active social media users.

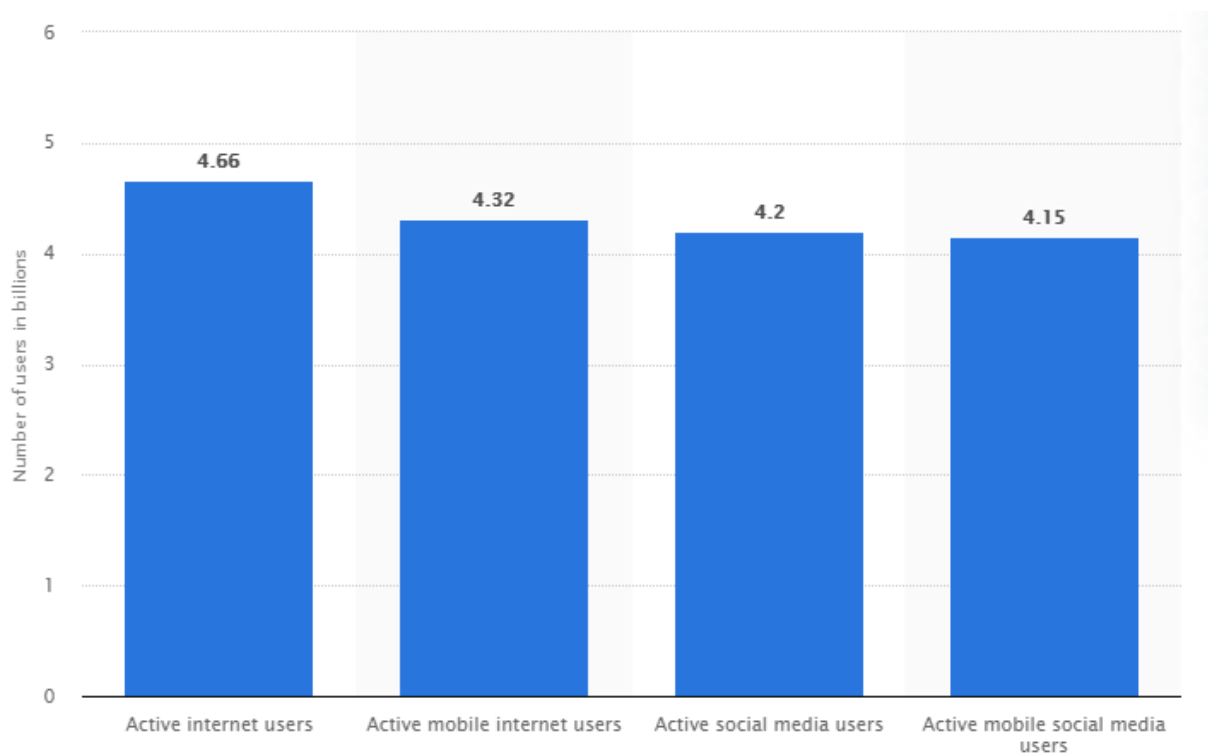
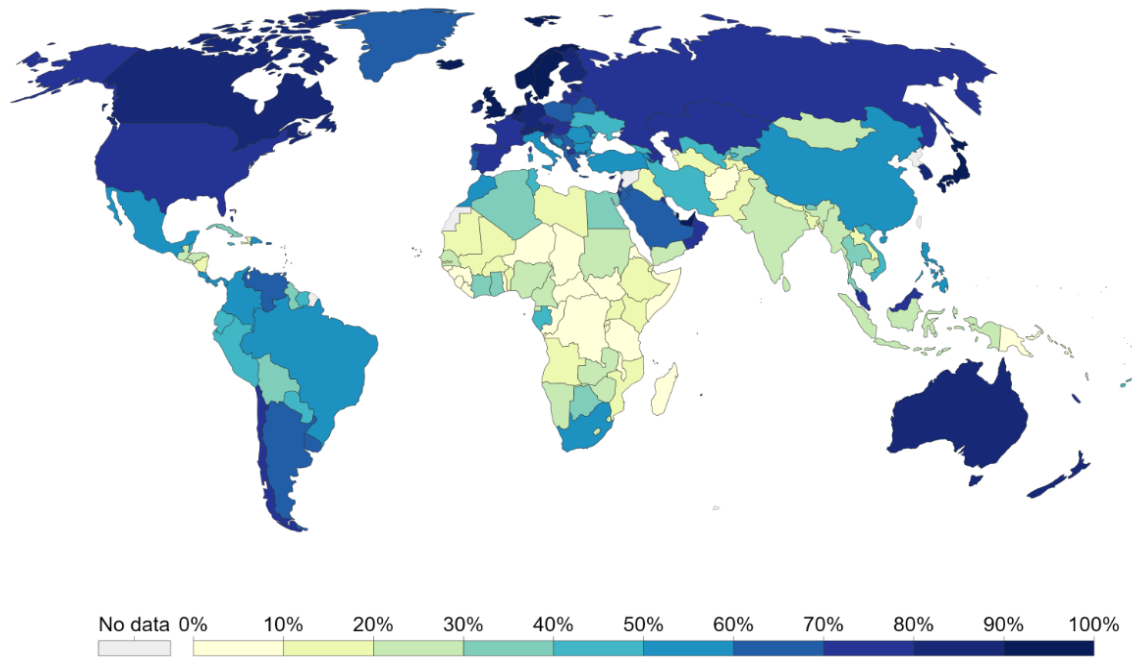


Figure 2. Global digital population as of January 2021 (in billions) (Statista, n.d.).

Some important challenges remain, however, and there is still work to do to ensure that everyone around the world has fair and equal access to life-changing digital connectivity.

Unfortunately, access to the Internet is far equal for all people (See Figure 3).





Source: World Bank

OurWorldInData.org/technology-adoption/ • CC BY

Figure 3. Share of global population using the Internet (Our World in Data, n.d.).

The map shows the share of the population that is accessing the Internet for all countries of the world. Internet users are individuals who have used the Internet (from any location) in the last three months. The Internet can be used via a computer, mobile phone, personal digital assistant, games machine, digital TV etc.

In richer countries, more than two-thirds of the population are typically online. And although usage rates are much lower in the developing world, they are increasing.

China and India take the top two slots despite having only 50 and 26 percent online, respectively. The top six countries by users (and the only countries with over 100 million) in 2016/2017 were:

1. China = 765 million;
2. India = 391 million;
3. The United States = 245 million;
4. Brazil = 126 million;
5. Japan = 116 million;
6. Russia = 109 million.

Unfortunately, the 4IR has risks as well, which especially has challenges for developing countries. One of the risks is related to eventual rising of joblessness.

Africa is a major producer of many key mineral commodities, with bountiful reserves of metals and minerals such as gold, diamond, cobalt, bauxite, iron ore, coal, and copper across the continent. Some of the major mining countries in Africa are the Democratic Republic of Congo (DRC), South Africa, Namibia, and Zimbabwe. In South Africa, around half a million workers are employed by the mining industry. If we are taking into count the possible full automatization of the mining industry, we could understand the size of the problem in the black continent.



New technologies threaten to strengthen and extend the already existing inequalities internally i.e., within the country and between countries. The 4IR has had certain other challenges, as well. One of them is the unethical issues in the public sector. Secondly, 52% of Africans covered by mobile broadband do not use it, mainly because of its high cost (Velluet, 2021).

That digital, mobile, and social media have become an indispensable part of everyday life for people all over the world. More than 4.5 billion people now use the Internet, while social media users have passed the 3.8 billion people. Nearly 60 percent of the world's population is already online (Kemp, 2021), and the latest trends suggest that more than half of the world's total population will use social media by the middle of this year.

### The Social Media's Influence on the Political Processes

Facebook, currently the largest and dominating social media platform in the world, has 2.4 billion users. Other social media platforms including YouTube and WhatsApp also have more than one billion users each.

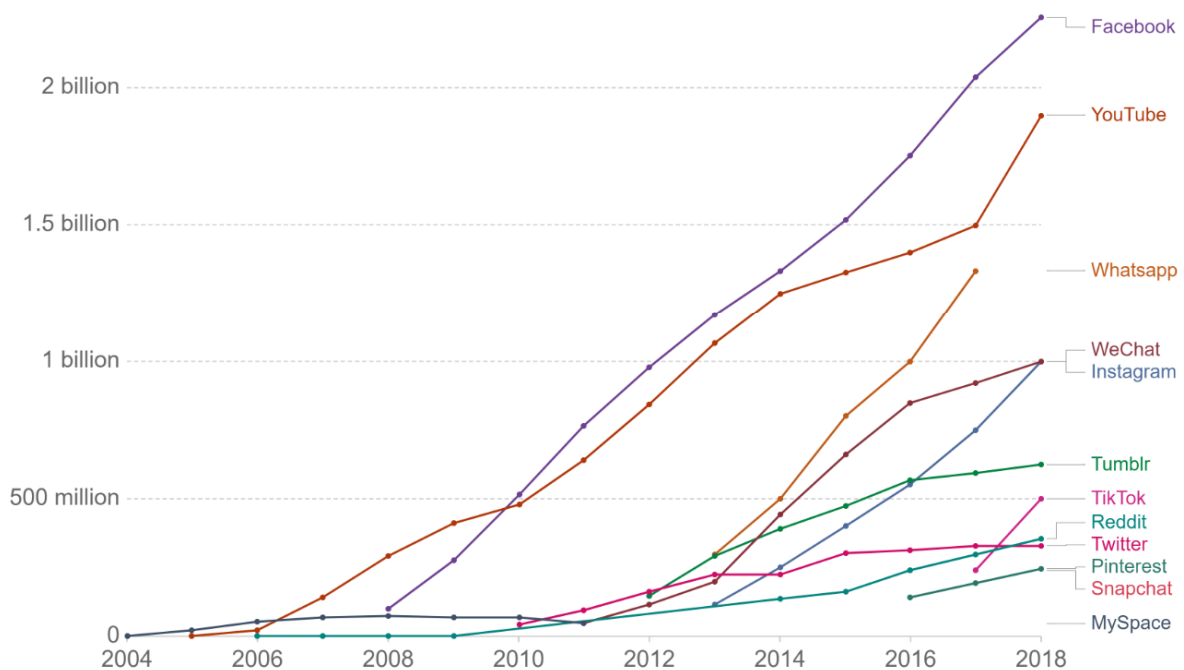
These numbers are huge—there are 7.8 billion people in the world, and almost half of it, 3.5 billion are online. This means social media platforms are used by one in three people in the world, and more than two-thirds of all Internet users.

Social media have changed and are changing the world, and more importantly, will influence in the future too. Facebook became a world power (See Figure 4). YouTube is also extremely popular.

The rapid and vast adoption of these technologies is changing how we find partners, how we access information from the news, and how we organize demand to political change.

#### Number of people using social media platforms, 2004 to 2018

Estimates correspond to monthly active users (MAUs). Facebook, for example, measures MAUs as users that have logged in during the past 30 days. See source for more details.



Source: Statista and TNW (2019)

CC BY

Figure 4. Number of people using social media platforms (Our World in Data, n.d.).



Following questions arise: Who uses social media? When did the rise of social media start and what are the largest sites today? Here we answer these and other key questions to understand social media usage around the world.

We begin with an outline of key trends and conclude with a perspective on the rate of adoption of social media relative to other modern communication technologies.

Social media's rate of growth in the US and other western countries, even in China and India is unimaginably high—in speed and to some extent also in reach—to that of most modern communication-enabling technologies, including computers, smartphones, and the Internet.

The rise of social media is an extraordinary example of how quickly and drastically social behaviours can change: Something that is today part of the everyday life of one-third of the world population was unthinkable less than a generation ago.

Facebook, YouTube, WhatsApp, WeChat, and Instagram are the top five social media platforms globally, with over one billion active users each. In the wealthiest countries, the proportion of young people using online social networks exceeds 90% and teens spend on average more than four hours online every day.

Fast changes like those brought about by social media always spark fears about possible negative effects. Specifically, in the context of social media, a key question is whether these new communication technologies are harming political and social issues.

In democratic countries with a sufficient system of checks and balances, the government is hindered to use social media for unfair political aims, such as spreading fake news about political rivals, expropriating online media for election campaigns, suppressing political programs of the opposite political side, etc. Never have such high-powered propaganda tools deployed in society.

Social media in well-functioning democracies can serve a better communication between the government and citizens, either in the political competition or in the decision-making processes of the government in certain issues, such as climate change, immigration policy, etc.

However, some autocratic governments, e.g., Russia or China, limit the access of citizens to the IoT to spread their one-sided approach, and to influence them. Hence, the citizens do not receive objective information; public opinion will be manipulated.

Autocratic governments often intervene in the political processes of other countries, too, e.g., Russia, by using social media.

The rights to keep sensitive data of individuals, e.g., religion, political view, race, etc., are often violated, when governments collect and use these data for their aims, e.g., to politically influence the citizens.

Social media in fragile states are often used to organize street demonstrations, riots, or revolutions against the government to fight for a more democratic and just society. This led e.g., to the development of the Arab Spring in the Islamic World.

In the events of Arab Spring, a revolutionary wave of demonstrations and protests in the Middle East and North Africa between 2010 and 2012, social media such as Facebook and Twitter played a significant role in facilitating communication and interaction among participants of political protests (Stepanova, 2011).

### **Advantages and Disadvantages of 4IR in the Political Sphere**

In democratic countries with a sufficient system of checks and balances, the government is hindered to use social media for unfair political aims, such as spreading fake news about political rivals, expropriating online



media for election campaigns, suppressing political programs of the opposite political side, etc. Social media in well-functioning democracies can serve a better communication between the government and citizens, either in the political competition or in the decision-making processes of the government in certain issues, such as climate change, immigration policy, etc.

People can express their opinion about public matters more easily, than by voting in the election, or public hearing to be held by a Member of Parliament (MP). People, in this way, feel more and more that their opinion counts in the political processes.

As disadvantageous effects of social media on politics should be noted when people form a social media group, e.g., in Facebook, Twitter, Instagram, etc., with those who are thinking in the same way but do not read good quality newspapers or watch political analyses or reports in the TV channels.

These phenomena do not encourage people to have other information than in their social media group, and they will not have information from other aspects, so, their political standpoints become on-sided. In worse cases, the so-called fake news and conspiracy theories spread dramatically in this way.

Just let's think of the evolvement of the pandemic of COVID-19 in 2020 all over the world, how many conspiracy theories spread in the social media about China or American billionaires who intentionally wanted to attack the West in this way or kill in quantities, elderly people. Fake news in social media announced that vaccines against COVID-19 are poisoned, aimed to kill people by conspirators. It has resulted that a significant part of the population in the countries is against the vaccines and challenges the governments in this way.

Those who did not get on vaccines hindered dissolving quarantines making the life of those who have already got on vaccines hard, and furthermore, promoted mutation of COVID-19 virus. This circumstance has led to further problems, such as the overwhelming health care system which cannot provide sufficient health care services for those who need them but are not with COVID-19.

It became urgent to liven up the slowed-down economy, which was the result of restrictions ordered by the governments because of the COVID-19.

Many lost their jobs, or many firms went to bankruptcy; consequently, the governments had to the fact of the growing number of unemployed. Governments were hesitating for a long time if to introduce law enforcement means, such as obligating people to get on vaccines, prohibiting people not getting on vaccines to enter public places, such as public transport, restaurants, movies, theatres, sports events, etc., or, obligating people who do not want to get on vaccines to pay for their health treatment related to COVID-19, pay higher insurance fees for this, or not to work, but stay at home.

Introducing these measurements means a political loss for the governments, but they are even forced to do because of public interest, such as to end spreading COVID-19, dissolving restrictions, giving jobs and income again for the people, stabilizing the health care system, restoring regular operation of the economy, etc.

In Hungary the government bought vaccines from China and Russia to have an even better political relationship with these two countries. These vaccines were not, however, approved by the Pharmaceutical Agency of the European Union, and the Hungarian government did not give sufficient information about these vaccines to the citizens. The opposition media revealed that the Chinese vaccine was not for the elderly above 60, because it did not give immunity for these people. This further pushed people to spread conspiracy theories in the social media why to be against vaccines.

The internet-based form of communications in crisis affected countries is often used as a platform for organizing public demonstrations. Social media platforms allow users to have conversations, share information,



and create web content in real time. This is a reason way the demonstrations, riots in Iran 2009-2010, and revolutions in Tunisia and Egypt got nickname of “Twitter Revolution” too.

It is especially important for the people to express their opinion in this way in autocracies and dictatorships, where certain human rights, such as freedom of speech, or the right to assembly are limited.

Another example can be mentioned in Hungary when social media had an important role to give sufficient information to people in an important public matter in an autocratic government system, where there is no access to public data.

It is already well-known that autocratic regimes like Turkey, Russia, and China, limit the access to internet. Russia after the invasion to Ukraine applied very strict regime against free social media and internet usage.

### **Using IoT by the Government to Manipulate Voters**

Governments can inform citizens by the Internet about public goals, their difficulties how to implement them, their results, etc., on the homepage of public authorities. Social media have changed this tradition of the Obama government that was established in the framework of the cloud computing project.

The government can establish a website, where citizens can ask about public matters, and give relevant information to their questions, e.g., about climate change, immigration, COVID virus, etc. Also, the citizen can write their opinion to the government about these issues. Based on the citizens’ questions, opinions, comments, governments can see if a proposed governmental decision is supported by most of the citizens, or not. Governments can easier and faster make conclusions in this way than to hold an expensive referendum.

Using IoT can serve transparency and accountability, when governments inform people about its operation, such as public tenders, its procedures, winners, or about the state budget, or local government budget.

The practices of the governments can strengthen democracy in the way of transparency, availability of public data, increase of accountability, better communication.

The other result of the cloud computing project introduced by the Obama government was the e-Government when citizens can arrange their administrative cases from home or in a public house, where everybody has access to the Internet. E-Government made public administration spectacularly efficient because citizens did not have to go to the public authority personally and stood in a long queue for a long time; also, business firms could decrease their costs in this way. In other words, e-Government using IoT can serve good governance, i.e., a more democratic political system, where the checks and balances system sufficiently work.

### **Misusing IoT by Governments to Manipulate Voters During Election Campaigns**

Using IoT evidently has several positive impacts on governance, but during the last decade, it has been a practice of populist governments to misuse and manipulate people and win elections.

It was Donald Trump in the United States that condemned the media accusing it of being biased, and began to inform the public about his ideas and thoughts by short messages using Twitter. This new habit of Donald Trump led to a practice in which he spread fake news to the public without any limitation or check. During the siege of the Capitolium in Washington D.C., in 2021, Donald Trump encouraged people to break into the building to fight for nullification of the election he considered falsified. His Twitter was blocked by the provider. This case shows that social media have not been under sufficient control, but it can spread fake news without any limitation.



When politicians and high-level government officials write fake news in their Facebook, Instagram, or Twitter, only the Internet provider can block these messages. It is the case even if Mark Zuckerberg the owner of Facebook was summoned in 2016 to the Congress of the United State to explain what measures he took to eliminate misuse of Facebook. Moreover, in the same year, Mark Zuckerberg apologized to EU lawmakers on Tuesday, saying the company had not done enough to prevent misuse of the social network and that regulation is “important and inevitable”. (It is well-known that in April 2018, the data-mining company Cambridge Analytica was able to harvest 87 million users whose personal information was accessed by a political consultancy that worked for Donald Trump’s presidential campaign.)

The other form of misusing IoT by politics is to spread fake news about political rivals, especially during election campaigns. The only way to defend from this is to sue those who wrote libels, but it takes time because legal procedures are long, longer than the election campaign that results from the election.

In dictatorships misuses of IoT are even much harsher than in democratic states. In Russia, e.g., special state-run clandestine institutions (it is in Saint Petersburg in Russia) established by the Russian government hire well-paid youth who speak foreign languages and spread fake news under false names of social media in Facebook, Twitter, or Instagram, about political candidates of election campaigns, who they do not want to win.

It had been proved by the CIA and the FBI in the United States that Russia intervened in the American election campaign in this way.

It was also revealed by the CIA and FBI that in 2006 the Russian government sent agents with falsified documents, e.g., passport, ID card, to the USA who opened Facebook as American citizens and especially in the competitive, disputed electoral districts (where the fight between presidential candidates seemed to be especially harsh), they spread fake news by joining social media communities, about Hilary Clinton who was the challenging presidential candidate of Donald Trump.

There has been a special Russian “invention”, the so-called “kompromat”, when the Russian government creates cases with the help of the agents of FSB (Russian Intelligence Service) or GRU (Russian Military Intelligence Service) to dox political enemies, especially during the election campaign.

This kind of “kompromat” has already appeared in Hungary in January 2022: Russia is politically interested in the winning of the recent governing party, the FIDESZ, organized by the FSB a case in which they provoked a conversation between businessmen close to the opposition parties and former officials of the Mayor’s Office, and intercepted it. Later, this recorded conversation was manipulated and reported on social media by an unknown man, “Anonymous”<sup>2</sup> whose face was covered by a hood. The aim of this “kompromat” was to discredit the mayor of the capital, Budapest, who is a leading politician of the alliance of opposition, which is the united opposition parties that have challenged the governing party, the FIDESZ in the election of 2022. The Mayor’s Office set up an ad hoc investigation committee to investigate the case, then it concluded it was a “kompromat” organized by the Russian intelligence service, the FSB, and this “kompromat” has been ordered by the Orban’s FIDESZ (Imre, 2021).

---

<sup>2</sup> Originally, “Anonymous” is a name of a decentralized international activist/hacktivist collective and movement widely known for its various cyberattacks against several governments, government institutions and government agencies, corporations, and the Church of Scientology already active from 2003. In Hungary, a FIDESZ guided Anonymous started to distribute some fake news for discrediting the opposition-led city council in Budapest in 2021. The real name of “FIDESZ Anonymous” up to now is unknown.



To reveal corruption cases and discrediting issues of the private life of politicians happened in another election campaign, too, i.e., in 2009 before the local government election. The “attorney-law of the devil” through the Internet (from an unknown website) revealed that a mayor of a Hungarian city participated in a sex-party with prostitutes in a yacht in the Adriatic sea. It was of course the violation of sensitive personal data, which is regulated as a crime by the Criminal Code, but the criminal investigating authorities could not find the persons who created this unknown website.

In Hungary, the recent government spreads its government propaganda by its media empire, e.g., the so-called Soros’ plan (Bauchamp, 2018)<sup>3</sup>, or the immigrant danger (Gorondi, 2019), and can successfully brainwash people. It is one of the reasons why the recent government could win the elections of 2014 and 2018: the government suppressed the opposition media step by step during the last 12 years, after they first had won the election with 2/3 majority, and did it by buying opposition newspapers, or withdrew licenses of Radio and TV channels. As a reaction to this media monopolization of the government, it has been a practice during the last decade that the opposition established online journals or broadcast on YouTube which cannot be quitted in any way.

A new phenomenon from the side of the Hungarian government is to use social media for this aim. An apparently independent non-profit organization was established at the beginning of 2022, to which a huge amount of money, more billions HUF was transferred by the government. This newly established non-profit organization, similar to the Russian “know-how”, hires many people to open Facebook, and spread government propaganda or fake news about opposition politicians, or it uses algorithms to manipulate users of social media by messages (Tibor, 2021).

Dictatorships, such as North-Korea, China, Russia quit the Internet, or limit its use by screening news, to hinder people to get objective information, and can prevent social unrest, street demonstrations, or riots.

### **Using 4IR Against State-Corruption**

E-Government can successfully prevent state corruption. If the government is obligated to publish public data about its operation, such as public procurements, state contracts, public money, salaries, and assets of politicians and public servants, corruption cases can be easily revealed. Its goal is to hinder state corruption with increasing accountability of politicians and public servants.

However, if the government is reluctant to provide public data when it is asked, the only opportunity is to sue the government. These forms are as follows: They do not send it electronically, but only copy the documents for extremely high fee. They select among the data, and do not submit the full documents, or delete some part of the document. Government often declares data asked from them to publish as a state secret for many decades to hide the information in this way. Court will decide these cases, and obligate government to publish public data. It on one hand is a long legal procedure; on the other hand, if the jurisdiction’s independency has been violated by the government, these legal cases will not be efficient to have access public data. This had been happening in Hungary since 2010, when the recent government won the election for the first time.

Hungary has been ceased to be a free country. Concerning the Bill on Protection Against Coronavirus, the Political Capital Institute stated that: “The remaining checks and balances in Hungary will cease to exist and

---

<sup>3</sup> The Orbán government between 2015 and 2017 launched a hysteria campaign against George Soros Hungarian origin US billionaire, former FIDESZ supporter because he wanted an open society in Eastern Europe. Moreover, the FIDESZ passed the so-called “Stop Soros” law.



the country will likely witness a new wave of attacks against the free press”. Some political analysts already some years stated that Hungary is not a democracy anymore but has been a so-called “illiberal democracy” with increasing autocratic feature (Szekeres, 2020). Hungary, according to the report of the Transparency International, has fallen to the worst place on the rank of state corruption of the member-states of the European Union. State corruption has been extremely high here: European Union sources disappear to the oligarchs of the governing party, or the friend and family members of the Prime Minister, Orbán.

OLAF, the investigation organization of the European Union, has already revealed several corruption cases that misuse EU funds, but the OLAF does not have the right to intervene in criminal procedures in member states, but only can report to the state attorney, who, in Hungary, is unwilling to open a criminal procedure the oligarchs and family members of the prime minister. Hungary has, in this way, become a hotbed of state corruption. Investigative journalists can successfully reveal these corruption cases of the government in Hungary, and publish them on social media, or, in YouTube, but only rarely with criminal consequences.

The non-democratic government often uses cyberattacks against state authorities, or high-level politicians to acquire sensitive information. In the American election campaign of 2006, the Russian government’s agents broke up the email of Hilary Clinton, the presidential candidate to discredit her with what she wrote in her correspondence. The same happened to President Trump’s children, who negotiated with a Russian attorney who offered them compromising information about Hilary Clinton. This latter case could not influence the election of 2006, because it turned out only after the election, but led to constitutional impeachment against President Trump.

### **Problems of Sensitive Data and the 4IR**

In democratic states, there must be an act on protecting personal data, especially sensitive data, such as race, political view, religious issues, health condition, criminal procedures, etc. The law on protecting personal data does not allow to publish personal data, or, to give it to unauthorized persons, or organizations.

To acquire personal data can happen in two illegal ways: In one case hackers break up the Internet system of a public authority, banks, or data of private users of the Internet. Sensitive personal data can be used against political enemies to discredit them. These cases cannot be revealed by criminal investigating means, due to the unknown website from where these data are spread in social media. The scandal of Pandora Papers in 2020 revealed the offshore bank accounts of leading politicians all over the world. In most cases of the last years, it is not known who the perpetrator was, not as in the case of Edward Snowden, or Julianne Assange? In 2021 the so-called Pandora Papers, the unprecedented leak of documents reveals the real owners of more than 29,000 offshore companies having a size of almost 3 TB (Ahmed, 2021). Millions of leaked documents and the biggest journalism partnership in history have uncovered financial secrets of 35 current and former world leaders, more than 330 politicians and public officials in 91 countries and territories, and a global line-up of fugitives, con artists, and murderers.

The PEGASUS scandal broke out in 2021 and revealed that governments bought spy software from an Israeli business firm to acquire information about journalists, politicians from their cell phones and email; however, the Israeli business firm stipulated in the sales contract that the spy software can be used only against terrorist to reveal their terrorist activities or organized crimes.

Countries are also developing new methods for data development and sharing such as the “World Statistics Cloud” that aims at improving the quality of information and reducing the costs of producing public data. In



public procurement, data mining is being used for auditing in order to monitor when governments are issuing bids and to identify red flags, patterns of collusion, and false information. Researchers at the Corruption Research Center Budapest have examined huge volumes of data sets of public procurement procedures from EU countries by searching for abnormal patterns such as exceptionally short bidding periods or unusual outcomes (e.g., no competition for the winning bid, or bids repeatedly won by the same company).

By going paperless, the governments can also tackle corruption and eliminate red tape. For example, in January 2019, Argentina became a paperless government, with the full digitalization of public administrative procedures. They also started to introduce the digital identity for all citizens, and they expanded the digital services. Artificial intelligence and predictive analytics are also potent tools for tax authorities and customs agencies to detect and deter tax evasion. Second, reformers in government can leverage new technologies to reduce the discretion that unscrupulous bureaucrats abuse to extract bribes, for instance in the processing of permits and licenses. The automation of bureaucratic processes reduces vulnerabilities to human fiddling.

There are numerous countries applying the technology of 4IR, where the leadership is trying to have more efficient public administration and governmental bureaucracies to make government leaner and smarter.

4IR to make public administration more efficient:

- Cloud computing by the Obama government;
- Against long queue and long wait: The client can arrange his or her administrative cases from home in a quick and flexible way. They can pay administrative fee, too, by an electronic finance system of the state budget, which is connected to cell phone or Internet;
- Poor people can use e-Government in public houses;
- Consumer can save energy (heating or lighting) in their homes by using smart applications;
- E-health services: Patients can get information of their examination, medical findings, lab diagnostic, from health institution via internet, and smart watch on old and sick people sends information to doctors from their homes, e-receipt;
- Home office during the pandemic.

Using IoT in the fragile states:

Unfortunately, we should recognize that the Internet can also be exploited by terrorists. While the many benefits of the Internet are self-evident, it may also be used to facilitate communication within terrorist organizations and to transmit information on, as well as material support for, planned acts of terrorism.

The Internet can be used for the glorification of terrorist acts, incitement to commit acts of terrorism, radicalization, and recruitment of terrorists, dissemination of illegal content, facilitating communication between terrorist actors, and the training of potential recruits. For example, the 9/11 actors used the Internet to collect information such as flight times; to communicate reliably and in real-time among themselves and with terrorist cells; to share information and coordinate their attacks, steal social security numbers, and obtain fake drivers' licenses. Moreover, the leader of the 9/11 attacks, Mohamed Atta, went online from Hamburg, Germany, to attend U.S. flight schools.

Despite the heinous nature of terrorist acts, alleged terrorists should be afforded the same procedural safeguards under criminal law as any other suspects. It is extremely difficult to determine the borderline between the expression of opinion (part of the basic human rights) and advertising terrorism (which is already a breach of criminal law).



Fragile states are safe heavens for the terrorist groups, because there is no public security, due to the lack of strong and efficient police and military, especially, when the country is full of a high rocky mountains, like Afghanistan, deserts, like Libya, or jungles, like Somalia. In the uncontrolled state borders, like in the countries of the Sahel in Africa, or in the border of Pakistan and Afghanistan in the Pashtun area, terrorists can easily change their basis, when they are in danger.

Terrorist groups can use the IoT for their aims:

- Terrorist leaders can give speech using the Internet from their hiding-place, how for example Osama bin Laden, or his successor, Ayman al-Zawahiri did it several times, announcing their aims of global jihad, or comment the situation in the Syrian and Iraqi war.
- When Abu Bakr al-Baghdadi, the former leader of the Islamic State (ISIS), claimed in Mosul in 2015? To be the caliph of the Islamic States (ISIS), it was announced by the Internet so that all over the world know it.
- The Islamic States made the best homepage for itself to advertise its terrorist activities and the life of the Islamic State in Iraq, Syria, and Libya, also, to recruit men to be the warrior of the Islamic State (ISIS), and young girls to be a wife of these warriors. Many warriors of the terrorist organizations from the Islamic world went there and joined the Islamic State (ISIS). Even more, it was so attractive for the young people in western countries who saw a good adventure in it that many two or third-generation young Muslims, or even Christians went from the developed countries of the European Union to join the Islamic State (ISIS).
- The Islamic State (ISIS) can successfully influence the two or third-generation young Muslims, who have problems with the integration into the western societies, and consequently, have an identity crisis, to radicalize and become a follower of the global jihad. Most of the perpetrators of the suicide terrorist attacks in western European countries, like France, Belgium, and Germany, in the last years, were from these so-called “lone wolves”.

Terrorists, however, do not use IoT in many cases to avoid being killed by combat drones but keep connection personally. Al-Kuwaiti, the messenger of Osama bin Laden, delivered messages to bin Laden personally to his house in Abbottabad. It took 10 years for the CIA to find this messenger, and through him, bin-Laden themselves.

Terrorists can successfully use the IoT to acquire security numbers, driving licenses, ID cards to have a false identity, like as happened in the case of 9/11. Israel developed the PEGASUS spy application (see above), by which they can intercept talks of the terrorists, or other devices by which they can target them with combat drones.

## **Conclusion**

Major technological achievements as the Artificial Intelligence (AI) may imply significant public policy issues. As electricity and other technical development did in the past, Artificial Intelligence (AI) is transforming our world today. There is no question that the potential to leverage Artificial Intelligence (AI) for positive change is enormous. On the other hand, government officials and political leaders cannot manage it alone. A task of this magnitude requires start-ups, medium, and large companies, and civil society—an entire GovTech ecosystem—function together to develop innovative solutions and improve outcomes. However, it is not only the ability of governments to be adapted to the new conditions. There are also severe social problems that may get bigger due to the Fourth Industrial Revolution making policy intervention extremely crucial.

It has been evident that openness and transparency is the best way to prevent corruption in the public sector because it makes state officials be more accountable for their decisions. In democratic governments, the IoT makes it an option for the citizens to have more information about government authorities.



However, what is working in the business world is not necessarily working in the public administration.

Nevertheless, if the government tries to hinder this right of citizens, e.g., with bureaucratic legal regulations, or forcing them to sue government authorities before the courts to give the data they asked, or if the government attacks those politicians, non-profit organizations, and journalists who reveal their corruption cases, these unfair attitudes of governments together with the insufficient operation of controlling authorities can easily lead to the hotbed of state corruption.

Advances in technology have led to unprecedented, rapid access to vast amounts of data on societies, the economy, and the environment. To keep up with this, governments, organizations, and citizens are in a new state of experimentation, innovation, and adaptation. The “data revolution”, which refers to both quantities of data now available and technological innovation, has the potential to tackle key issues in society including corruption.

Traditionally it has been difficult to expose corruption due to large quantities of data. However, digitalism and the popularity of big data have led to new data management techniques to prevent fraud and abuse in the public sector. In underdeveloped countries, especially in some African countries, rapidly improving access to electricity should be a key policy priority. Governments should view energy security as a function of investment in renewables and the foundation for future growth.

The proliferation of technology of 4IR (big data for capturing, data mining for detecting, mobile applications for increasing accessibility, and forensic tools for reducing opportunities for corruption) has the potential to create unparalleled opportunities for transparency and anti-corruption. However, technology is not a quick fix or fast solution because of the need for financial investment into the public administrative sector, plus the need for an adaptation to new technology.

The technology of 4IR has become transparency’s greatest ally to anchor integrity in the public sector. Coupled with political resolve, the digital revolution can disrupt corruption in ways we never imagined possible.

Several countries are trying to streamline their bureaucracies to make government leaner and smarter. This is no small challenge, as it requires a shift in mindsets for bureaucracies to serve citizens, rather than the other way around.

The emergence of GovTech start-ups is allowing new forms of co-creation of public administrative services, especially at the local level. These smaller, more agile companies are starting to make an impact, advancing new solutions to old ways of doing things. The GovTech applications are also helping to transform government and, in some cases, challenging the state’s monopoly over the delivery of services. For example, they provide a cost-effective solution to data-analytics-as-a-service to governments that are struggling to recruit data science teams. Unfortunately, the technology of the Fourth Industrial Revolution has a double face. The phenomena of global terrorism and organized crime can emerge due to highly advanced technology which can cause slavery of children and other vulnerable groups of people in communities due to unscrupulous fortune promising online platforms. It is argued here that all governments need to be ready to adapt to the challenges represented by the Fourth Industrial Revolution.

## References

- Ahmed, T. B. (3 October 2021). Offshore havens. *International Consortium of Investigative Journalism*. Retrieved from <https://www.icij.org/investigations/pandora-papers/global-investigation-tax-havens-offshore/> (accessed on 02/02/2022)
- Bauchamp, Z. (2018). Hungary just passed a “Stop Soros” law that makes it illegal to help undocumented migrants. Retrieved from <https://www.vox.com/policy-and-politics/2018/6/22/17493070/hungary-stop-soros-orban>



- Golan, G. J., Arceneaux, P. C., & Soule, M. (2019). The Catholic Church as a public diplomacy actor: An analysis of the pope's strategic narrative and international engagement. *The Journal of International Communication*, 25, 95-115.
- Gorondi, P. (2019). Hungarian PM Orban launches campaign with anti-migrant plan. Retrieved from <https://apnews.com/article/ddff4e9c32f74ffcac4fee3907a7f1e5> (accessed on 02/02/2022)
- Imre, C. (2021). Karácsony Gergely: A hazug, manipulált hangfelvételek mögött a Fidesz áll. Retrieved from <https://index.hu/belfold/2021/11/19/karacsony-mar-az-orosz-titkosszolgalatot-sejti-a-varoshaza-ugy-mogott/> (accessed on 02/02/2022)
- Kemp, S. (2021). 6 in 10 people around the world now use the internet. Retrieved from <https://datareportal.com/reports/6-in-10-people-around-the-world-now-use-the-internet> (accessed on 26/06/2021)
- Our World in Data. (n.d.). Internet. Retrieved from <https://ourworldindata.org/internet> (accessed on 16/06/2021)
- Shank, P. (March 30, 2016). 2025: How we will work? How will your job change? Association for Talent Development. Retrieved from <https://www.td.org/insights/2025-how-will-we-work-how-will-your-job-change+> (accessed on 26/06/2021)
- Statista. (n.d.). Global digital population as of January 2021. Retrieved from <https://www.statista.com/statistics/617136/digital-population-worldwide/> (accessed on 27/06/2021)
- Stepanova, E. (May 2011). The role of information communication technologies in the "Arab Spring" implication beyond the region. *PONARS Eurasia Policy Memo No. 159*.
- Szekeres, E. (31 March 2020). Unlimited emergency powers granted to Prime Minister Viktor Orban have taken Hungary a step closer to dictatorship. Retrieved from <https://balkaninsight.com/2020/03/31/hungary-no-longer-a-democracy-after-coronavirus-law/> (accessed on 02/02/2022)
- Tibor, L. (2021). Már 41 milliárd ment el Nemzeti Konzultációra. Retrieved from [https://hvg.hu/itthon/20210903\\_Nemzeti\\_konzultacio\\_41\\_milliard](https://hvg.hu/itthon/20210903_Nemzeti_konzultacio_41_milliard)
- Velluet, Q. (2021). Three ways Africa's digital economy can improve in 2021. Retrieved from <https://www.theafricareport.com/57242/three-ways-africas-digital-economy-can-improve-in-2021/> (accessed on 26/06/2021)
- Zhuravskaya, E., Petrova, M., & Enikolopov, R. (2020). Political effects of the internet and social media. *Annual Reviews of Economics*, 12, 415-418. Retrieved from <https://www.annualreviews.org/doi/10.1146/-annurev-economics-081919-050239> (accessed on 02/02/2022)