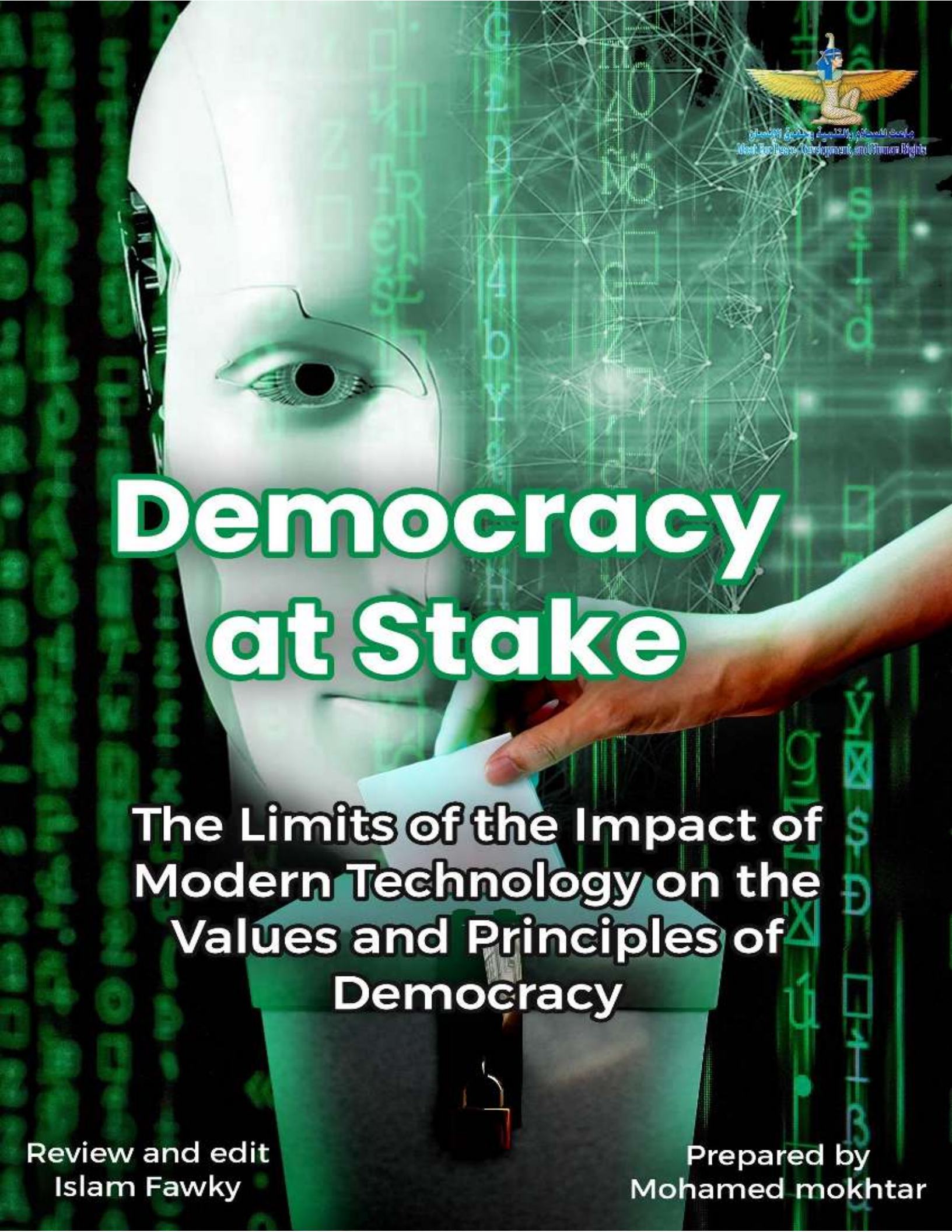
Democracy
at Stake
The Limits of the Impact of Modern Technology on the Values and Principles of Democracy
Review and edit
Islam Fawky
Prepared by
Mohamed mokhtar

Executive Summary

Modern technological applications have brought about unimaginable changes in people's daily lives; however, these applications came with grave threats and implications to democracy. They are heavily employed to violate citizens' personal rights, limit their political participation in the public field, undermine election integrity, place political opposition, civil society organizations, and free media under spotlights, along with exacerbating inequality in societies, and undermining the rule of law, which violates many international human rights instruments, including the International Covenant on Civil and Political Rights.

At the top of these technologies are the AI-enabled applications, digital espionage tools, and applications used in malicious cyber-attacks, let alone social media as one of the modern digital tools. On the occasion of the International Day of Democracy corresponding to September 15 of each year, Maat for Peace, Development and Human Rights presents this study to highlight the impact of modern technological applications on the principles and values of democracy. Maat opens the study by highlighting the status of democratic values in the digital age and then moves forward to discuss the impact of these technologies on the state of democracy and its principles and values. Maat concludes the study by presenting a set of recommendations with the aim of correcting the path of democracy in the era of new technologies so that the values of freedom, equality and respect for human rights prevail worldwide.

Study Methodology

The study was based on a set of general, measurable and observable indicators, to determine the impact of modern technologies on the values and principles of democracy, with reference to many international treaties and instruments, particularly the International Covenant on Civil and Political Rights. The study also relied on a review of literature and studies published on the website of the Office of the High Commissioner for Human Rights, as well as studies and news issued by independent human rights centers, which intended to analyze to reach these indicators, which have been divided into five main indicators that include a number of sub-criteria, and they can be mentioned as follows:

Individual Freedoms Indicator: this indicator relates to governments' use of new digital technologies to suppress individual freedoms with regard to democratic values, which can be deduced through governments' use of technologies aimed at monitoring

public affairs and individual freedoms, in addition to the sponsorship of governments to smear campaigns launched against human rights activists and oppositions, and their use of the internet to spread disinformation discourses that put individual freedoms under siege.

Elections and Voting Indicator: this indicator depends on the use of digital technologies to influence electoral systems and voting processes, negatively impacting the right of citizens to manage public affairs and limiting their ability to choose their representatives in free elections. This is measured by knowing the extent to which digital technologies are used to fabricate statements of political officials and party leaders during elections, with the aim of manipulating public opinion and falsifying elections and their lack of integrity, as well as relying on the collection and manipulation of user data in order to predict and influence the political opinions of voters and election results.

Rule of Law Indicator: this indicator assesses judicial systems that rely on technology in the field of criminal justice, by measuring the extent of bias and unfairness in the applications of the technology used in various criminal investigations, in the automation of decision-making processes related to areas of criminal justice, and the its relation to achieve the rule of law.

The Independence of Civil Society Organizations and the Media Indicator: this indicator depends on evaluating the work of civil society organizations in the digital environment, and the extent to which they are allowed to carry out their activities without harassment in cyberspace. Such harassment may be electronic attacks or campaigns to discredit the opposition.

Political Participation Indicator: this indicator shows the extent to which new technological applications affect citizens' participation in public affairs. This can be inferred by knowing how countries use social media to change political discourse, distort public opinion, and limit and undermine citizens' participation in political discussions, in addition to other obstacles made by the government to ensure that information does not reach the public in the most transparent manner.

An overview of the status of democratic values in the digital age

Many international human rights instruments stipulate a set of values and principles that constitute in essence the general framework of the democratic process,

topped by the need to respect the individual rights of citizens, organize periodic, free and fair elections, as well as promote political and public participation in societies, and respect the principle of the rule of law. In addition to accountability for all those holding a public position, strengthening the principles of equality between all groups, in addition to establishing and supporting transparency at all levels of society. At the same time, achieving these elements requires the presence of strong and independent civil society organizations, with media characterized by pluralism and freedom to present different opinions[1].

During the past few years, the emergence of many new technologies has negatively affected the values of democracy, as these technologies have become a serious threat to the individual liberties of citizens, not to mention their impact on the integrity of elections by manipulating the voting behavior of individuals, and their ability to undermine the political participation of citizens. These technologies also help to fuel inequality among citizens at unprecedented levels, and places civil society institutions and the media under constant scrutiny, so that their members exercise self-censorship on themselves. This situation is made worse by the presence of tech giants operating in regions devoid of democratic values, without the ability of governments to hold them accountable for their illegal activities[2].

Many evidence points to the role played by artificial intelligence applications in manipulating information, particularly on social media, which in turn affects the participation of citizens in elections, contributes to the suppression of many individual freedoms of citizens, and reduces the rule of law through artificial intelligence biases in the fields of criminal justice[3]. However, modern electronic espionage software threatens individual freedoms on a large scale, undermines the independence of civil society organizations and the media, and allows the ongoing prosecution of activists and human rights defenders, in an environment that does not provide the minimum standards for respecting basic democratic values[4].

On the other hand, cyber-attacks contribute to consolidating the capabilities of authoritarian governments by limiting the effectiveness of independent media, suppressing political opposition, persecuting civil society organizations, negatively

---

[1] الديمقراطية، الأمم المتحدة ، https://bit.ly/3erjKMX

[2] Many Tech Experts Say Digital Disruption Will Hurt Democracy. Pewresearch. https://pewrsr.ch/3Qnu0mC

[3] ما بين التهديد والتعزيز كيف سيؤثر مستقبل الذكاء الاصطناعي علي حقوق الإنسان، ماعت للسلام والتنمية وحقوق الإنسان، https://bit.ly/3tnrbcR

[4] فضيحة برنامج بيغاسوس هل أصبحنا جواسيس دون أن ندري؟ ، بي بي سي العربية ، يوليو ٢٠٢١، https://bbc.in/3qcJZJt

affecting democratic elections and questioning their integrity, thus consolidating their authoritarian anti-democratic approach at the global level. Social media, as one of the new technological techniques, raises controversy about its use by multiple parties to manipulate information to the detriment of the political participation of citizens, as well as being a tool at times for disinformation and defamation campaigns targeting political oppositions, human rights activists, and civil society organizations[5].

Digital Threats: Risks of AI-Enabled Applications to Democracy

There are many negative repercussions resulting from the heavy reliance on AI technologies in all aspects of life; topped by the ability of these applications to destabilize the basic principles of democracy. On the level of individual freedoms, the security services use facial recognition technology to monitor, track, and identify demonstrators during public protests to arrest them[6]. In August 2020, during the protests condemning the killing of George Floyd in the United States of America, the security services, in a number of American states, used facial recognition technology to arrest a large number of demonstrators, despite the law stipulating that it is not permissible to use facial recognition technology to monitor people engaged in constitutionally protected activities such as peaceful protests[7]. In December 2019, Indian police in the northern state of Uttar Pradesh used the same technology, and arbitrarily arrested protesters during protests that erupted after the adoption of a new citizenship law that marginalizes the status of Muslims in India[8], which contravenes Article 21 of the International Covenant on Civil and Political Rights, which confirms that the right to peaceful assembly is one of the most important components of democratic societies[9].

Facial recognition technology also threatens a person's right to privacy related with the basic individual freedoms necessary to establish a democratic society and enshrined in the International Covenant on Civil and Political Rights[10]. Many human rights estimates indicate the Chinese government’s exploitation of facial recognition technologies to monitor the movements of ethnic and religious minorities, especially the Uyghurs and Tibetans[11], while other artificial intelligence technologies were used

[5] Like War – The Weaponization of Social Media. https://bit.ly/3cO9IVL

[6]

[7] Miami Police Used Facial Recognition Technology in Protester's Arrest. **nbcmiami.** August 17, 2020. https://bit.ly/3DgeuGv

[8] India's use of facial recognition tech during protests causes stir**. reuters**. February, 2020https://reut.rs/2R9UYVZ

[9] الدليل الإرشادي حول العهد الدولي الخاص بالحقوق السياسية والمدنية، مركز تطوير المؤسسات الأهلية ، https://bit.ly/3wXfBH2

[10] الدليل الإرشادي حول العهد الدولي الخاص بالحقوق السياسية والمدنية، مرجع سابق ذكره

[11] Religious Freedom in China’s High-Tech Surveillance State. Uscirf .https://bit.ly/3cQh7kD

during the spread of the Covid 19 epidemic to limit individual freedoms. An Israeli company, affiliated with the government, developed a system to analyze faces relying on deep learning technology to eventually be able to identify those infected with the Coronavirus[12], while the Israeli company Any Vision is working on developing models of artificial intelligence applications that allow mass monitoring of citizens in Palestine[13].

On the other hand, AI applications have become more capable of spreading fake news, misleading propaganda and manipulative information, which affect the right of citizens to form their opinions and receive information, and disrupts their ability to choose between candidates during elections, which would undermine the integrity of elections, limit levels of political participation, and affect the credibility of the media[14]. As such, the 2016 US presidential elections demonstrated the ability of many countries to take advantage of robots and artificial intelligence-based social media algorithms, to increase the reach of false information and potentially influence voters, which contributed to undermining political participation and loss of confidence in democracy[15]. Many estimates prohibit the ability of the deep forgery technique to have an unprecedented impact on elections and the ability of citizens to choose who represents them, which raises serious questions about the integrity of democratic elections. Deep forgery technology has the ability to fabricate politicians' statements, create fake scenes of violence, and publish them through social media, which negatively affects voters' attitudes during elections[16].

Many judicial systems worldwide have begun to use AI applications in the field of criminal justice, in order to support judges in predicting various sentences. Police agencies resort to algorithmic tools related to artificial intelligence to determine future criminal behavior and predict the level of crimes, but the bias of artificial intelligence systems contributed in threatening the rule of law, as decisions about the risk assessment of crimes, and the prediction of the likelihood of being committed in the future, are often biased against people of color, there are many facts that bias Artificial Intelligence decisions towards people of African descent in the field of criminal justice in the United States of America[17].

---

[12] تقنيات تكشف عن رائحته وصوته. إسرائيل تواجه كورونا بتكنولوجيا القتل والتجسس، الجزيرة، يونيو 2020 https://bit.ly/31PY3MS

[13] كيف تستخدم إسرائيل الذكاء الاصطناعي بالتعاون مع مايكروسوفت لمراقبة الفلسطينيين؟، الأخبار الأوروبية ، أكتوبر 2019 ، https://bit.ly/2PYrGc8

[14] The Impact of Artificial Intelligence on Human Rights, Democracy and the Rule of Law. ALLAI. March 20, 2020 . **https://bit.ly/39GO7cQ**

[15] Deepfakes and the 2020 US elections: what (did not) happen. Arxiv. https://bit.ly/3AQ4tNd

[16] التهديد المتصاعد لـ"الخداع العميق" عبر نظم الذكاء الاصطناعي، مركز المستقبل للدراسات السياسية والاستراتيجية ، ديسمبر 2019 ، https://bit.ly/3miTXGH

[17] كيف يمكن لتطبيقات الذكاء الاصطناعي أن تكون متحيزة، مسار ، سبتمبر ٢٠٢١ ، https://bit.ly/3qbyLVB

The risks of Artificial Intelligence bias also lie in exacerbating racial discrimination and perpetuating inequality in many areas, particularly gender-based discrimination, while reinforcing gender and racial stereotypes, thus eliminating the principles of equality and justice that underpin democratic systems[18].

Control Obsessions: Spyware Limits Democratic Values

Many governments around the world have used spyware and surveillance tools that violate all democratic values. These dangerous and complicated software allow governments to spy on civil society activists and oppositions by reading the contents of their e-mail correspondence, in addition to cascading all their online activities, by remotely and invisibly accessing their personal devices and turning on the device's microphone, camera, or GPS-based positioning technology without the victims' knowledge of this matter, in addition to the ability of governments to manipulate the data on these devices, by deleting or destroying data or transplanting misleading data, in some cases develops into secretly monitoring the recording of their personal activities and threatening them with the aim of silencing their mouths to prevent the disclosure of the horrific violations of human rights committed by these governments. All of these pose serious threats to individual liberties, as well as to human rights defenders and political oppositions, which are one of the fundamental values of democracy[19].

In January 2022, human rights estimates revealed that the government of El Salvador had used Pegasus spyware to target journalists and human rights defenders[20]. In October 2021, documented information indicated that the Israeli occupation government had used a number of spyware to target and monitor 75 iPhone devices owned by a number of human rights defenders and political activists defending the Palestinian case. It is worth noting that the Israeli occupation government had a precedent in dealing with the Israeli company Elbit, which provided the government with tools to monitor Palestinian civil society in 2019[21]. Moreover, the Spanish government was pressured by the opposition, demanding it to provide explanations about the subjection of oppositions, linked in one way or another to the movement

[18] ذكاء اصطناعي بملامح البشر مخاطر التحيز والأخطاء في الذكاء الاصطناعي ، مركز راند، https://bit.ly/3CZo6F7

[19] Use of spyware to surveil journalists and human rights defendersStatement by UN High Commissioner for Human Rights Michelle Bachelet. OFFICE OF THE HIGH COMMISSIONER FOR HUMAN RIGHTS. https://bit.ly/3RBAQGf

[20] Pegasus attacks in El Salvador: spyware used to target journalists and activists. Accessnow. JANUARY 2022. https://bit.ly/33yAHjl

[21] برامج تجسس تستهدف مدافعينات فلسطينيات عن حقوق الإنسان، مؤسسة الضمير لرعاية الأسير وحقوق الإنسان، أكتوبر 2011 ، https://bit.ly/36tsXjV

separatists in Catalonia, to penetration through the Pegasus program in the period from 2017 to 2021.[22]

The government in Togo also targeted opposition websites with spyware using technologies it obtained from Israel. Social justice activist and Catholic priest Pierre Marie Chanel Avonon was also subjected to Pegasus' surveillance as part of the government's iron grip in Togo on civil society[23]. In Hungary, the government was implicated in spying on at least 300 journalists, civil society activists, and government opponents using the Israeli NSO company's Pegasus tool, including human rights journalists Szapolos Banje and Andras Szabo, in addition to the journalist "David Derxini" and some other businessmen who were not mentioned[24].

On the other hand, the Israeli digital intelligence company Cellebrite has been implicated in selling products and services to countries that facilitate mobile phone tracking and other devices; especially for political activists and human rights defenders bypassing their passwords and encryption and extracting data. The Universal Forensic Extraction Device (UFED) is sold in more than 150 countries worldwide. For example, in April 2020, the government in Botswana used this tool to obtain information about incriminating human rights journalist Ortayl Dikologang. However, the Myanmar government used the same tool to prosecute Reuters journalists "Wa Lone and Kyaw Soe" for their human rights reporting on human rights violations against the Rohingya Muslim minority across the country[25].

In Asia, governments are increasingly relying on cyber-espionage technology to reveal information about civil society activists and leak it online to exposes them to the risk of societal stigmatization and to force many of them to remain silent about violations committed by the government. In Azerbaijan, more than 100 devices and electronic phones have been targeted for dissidents, human rights activists, and their families, including Khadija Ismayilova phone, the most famous investigative journalist in Azerbaijan. She was targeted by the Pegasus spyware program to obtain personal information about her[26]. The government leaked photos of many civil society activists to stigmatize them after entering their phones through various malware. Among them are civil society activist and journalist "Fatima Muflamli" whose intimate photos were

[22] هل عزل رئيسة الاستخبارات الإسبانية بسبب فضيحة التجسس.. عملية تهدئة لبقاء الحكومة اليسارية في السلطة متاح على الرابط https://bit.ly/3N2YuJX

[23] Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries .https://bit.ly/3l4XzO3

[24] هل يواجه المجر عقوبات أوروبية بسبب تسريبات "بيغاسوس"؟، درج، https://bit.ly/3eS27Dl

[25] What spy firm Cellebrite can't hide from investors. Accessnow. MAY 2021. https://bit.ly/3sQkSNz

[26] تسريبات "بيغاسوس"- آذربيجان: صندوق حديد ربما يحمي خديجة من التجسس، درج ، https://bit.ly/3faPuDJ

leaked on the social networking site Facebook in 2019 with insulting expressions of her, which exposed her to societal stigmatization[27].

India has also used Pegasus to spy on public figures, including Prime Minister Imran Khan[28]. The exiled leader based in India, the Dalai Lama, was also spied on. Moreover, in July 2021, the political opposition staged protests calling for serious investigations into the Indian government's use of Pegasus software to target political opposition across the country[29]. Spying on the political opposition limits its effectiveness and seriously undermines democracy.

Destabilization: The Consequences of the Increased Exploitation of Cyber Attacks on Democratic Values

Cyber attacks play a role in undermining trust in official government institutions by tampering with or destroying data, providing the opportunity to question the legitimacy of elections, and manipulating the voting behavior of citizens. Attacks on electoral systems affect the democratic rights of representation of citizens who are denied their right to vote. However, targeting civil society organizations with more cyber attacks harms the entire democratic process due to the importance of these organizations in preserving the different values of democracy.

Many parties are exploiting cyber-attacks as a tool to limit the legitimacy of elections and question their integrity. In September 2021, the body supervising the general elections in Germany website was subjected to denial of service attacks and denial of service attacks a few weeks before the elections that took place on September 26, 2021[30]. That is not the first time that elections in Germany have been targeted. In January 2021, cyber-attacks against the Christian Democratic Union's website increased to undermine its chances of winning elections and questioning its legitimacy. That poses a threat to the electoral process and the voting rights of citizens in Germany[31].

On the other hand, civil society organizations and human rights activists are facing an increasing range of cyber attacks from phishing and denial of service attacks.

---

[27] Pegasus project: spyware leak suggests lawyers and activists at risk across globe .https://bit.ly/2TAtuug

[28] باكستان تدعو الأمم المتحدة للتحقيق في استخدام الهند برنامج "بيغاسوس للتجسس، https://bit.ly/3ryY184

[29] الهند: تظاهرات مطالبة بالتحقيق في فضيحة برنامج التجسس "بيغاسوس"، https://bit.ly/36VWlw2

[30] هجوم إلكتروني يستهدف موقع هيئة الانتخابات الألمانية، الشرق ، https://bit.ly/3et49wn

[31] الهجمات الالكترونية تلقي بظلالها على الانتخابات الألمانية، تي دبيلو نيوز ، https://bit.ly/3cNWM1Z

To practice revenge against them for their human rights work or force them to remain silent about the various human rights violations. That harms many civil and political rights stipulated in the International Covenant on Civil and Political Rights. Among them is the right to form associations stipulated in Article 22 of the Covenant[32]. Civil society organizations are considered one of the most important pillars of the democratic process and consequently, restricting them is considered a direct attack on the values of democracy.

On June 17, 2019, many attempts were made to hack the social media and email accounts of the human rights organization PROMEDEHUM[33], a prominent civil society organization in Venezuela. In 2018, with the start of the presidential elections in Azerbaijan, the government, with the help of its affiliate groups, undermined the work of civil society organizations opposing it on the Internet through cyber attacks. Some human rights organizations have been subjected to direct denial of service attacks not only but some opposition media websites were subjected to electronic penetration and the removal of all information available to them. The personal Facebook account of the Azerbaijani human rights activist "Jamil Hasanli" was also hacked, with all his followers deleted. [34] Civil society organizations and activists In Vietnam have had their online accounts taken over. And that is through cyber-attacks based on fake links and loaded with malware that violates the digital security of the Internet user to access their account information[35].

Information manipulation: Social media as a tool for spreading hate speech

Many countries have been involved in disinformation campaigns to discredit political opponents, attack human rights activists, and blur the facts, using social media as an essential tool to achieve this. These campaigns directly affect election campaigns by manipulating information and spreading false news.

Official reports and estimates issued by the US government indicate that the Russian government interfered in the 2016 US presidential elections, which were held between Republican candidate Donald Trump and Democratic candidate Hillary Clinton. The Russian government has supported Republican candidate Donald Trump due to political and ideological considerations in the interest of Russian President

[32] الدليل الإرشادي حول العهد الدولي الخاص بالحقوق السياسية والمدنية، مرجع سابق ذكره

[33] CYBER ATTACKS AGAINST HUMAN RIGHTS ORGANISATION PROMEDEHUM .Frontlinedefenders .https://bit.ly/30mnKan

[34] Azerbaijan's authoritarianism goes digital،meydan،February 2018،https://bit.ly/3BPHyAP

[35] Vietnam under review at the Human Rights Council: Cyber attacks on civil society a key concern .Ccessnow .https://bit.ly/3FLBv2C

Vladimir Putin. By manipulating information published online about Hillary Clinton and supporting her Republican counterpart. Several Russian groups also used strategies to spread and promote false news about the Clinton campaign, in addition to manipulating the contents and American minds and undermining access to information[36].

For example, Russian groups funded about 1,800 tweets in support of the US president in the form of hate speeches targeting the rival candidate[37]. This incident resulted in a violation of citizens' right to access information and the right to freely hold opinions enshrined in Article 19 of the International Covenant on Civil and Political Rights. That refers to the right of citizens to seek, receive and impart information and ideas of all kinds, which requires not manipulating opinions unintentionally or influencing them involuntarily. However, the dissemination of fake news stories on social media by Russian groups completely ignored this article and even violated the rules of the democratic process[38].

The Russian government carries out fake news campaigns that lasted between 2015 and 2017 across Europe to achieve its political goals. It worked to influence the results of the Polish presidential elections in 2015 and supported the fortunes of the right-wing candidate Marine Le Pen at the expense of Emmanuel Macron, but the estimates succeeded the latter. However, this does not negate the human rights violations that occurred[39].

On the other hand, Iranian government groups have tried to undermine the right of citizens in America to express their opinions. In addition to the right to participate in public affairs and elections enshrined in Article 21 of the International Covenant on Civil and Political Rights, during the preparatory period before the 2020 presidential election. Propaganda videos were published about election fraud and hacking of American voter information and showing the voting process is unsafe and vulnerable to fraud to support the candidate Democrat Joe Eden at the expense of his Republican counterpart[40].

---

[36] الانتخابات الأمريكية 2020 مايكروسوفت تتهم قراصنة من روسيا وإيران والصين باستهداف الاقتراع، بي بي سي العربية ، سبتمبر 2020 ، https://bbc.in/3klvoGA

[37] تويتر 1800 تغريدة روسية للتأثير على نتائج الانتخابات الرئاسية الأمريكية، فرنسا 24 ، ديسمبر 2017 ، https://bit.ly/3iWnUfj

[38] العهد الدولي الخاص بالحقوق المدنية والسياسية، مكتبة منيوسوتا، http://bit.ly/31BW3p0

[39] How do you solve a problem like troll armies? .Accessnow .https://bit.ly/2YJb0ue

[40] مسؤولون أميركيون إيران تزوّر مواقع إعلامية للتأثير في الانتخابات، الحرة ، أكتوبر 2020 ، https://arbne.ws/3AwxGuh

Human rights defenders, journalists, and politicians face widespread verbal abuse and defamation on social media through disinformation campaigns. Social media manipulation has become part of the business of governments as their internet mercenaries denigrate opponents with moral and patriotic claims by branding them as treasonous or immoral. That undermines confidence in their statements among the general public and lose their influence over digital media[41].

The Iranian government has used online groups affiliated with it to undermine confidence in the opinions of human rights activists, in addition to forcing them to remain silent and imposing self-censorship on themselves. A large number of activists are accused of working for defamation of their names, which facilitates the task of liquidating them in the future. In Iraq, many individuals affiliated with the Popular Mobilization Forces loyal to the Iranian government are attacking human rights activists with false information that leads to targeting them and threatening their lives. All accounts that spread misinformation about activists bear the same style and format and spread the same message[42]. Perhaps the most tangible result of these campaigns is the assassination of Iraqi activist Reham Yaqoub in August 2020 because of the electronic disinformation she was exposed to[43]. Iraqi activist Lodi Raymond Alberti was also subjected to a smear campaign on social media. After she was assassinated by unknown armed groups, many of the Iranian government's electronic brigades promoted a false narrative alleging that the activist was attempted murdered by her family members in an honor crime[44]. That leads to a distortion of its reputation and its legitimate work in the defense of human rights. This campaign also forced her to leave her home city of Basra for fear of persecution and social stigma.

In Lebanon, the situation is not much different. In January 2021, the media on the Al-Hurra TV channel, the Nights of Choice, was subjected to a campaign of incitement, treason, and death threats that included many false statements. That was against the background of publishing a tweet criticizing Hezbollah's erection of a statue of Qassem Soleimani and citing a Quranic verse about the statues by people affiliated with the pro-Iranian Hezbollah. As such, the use of systematic online disinformation campaigns by mercenaries affiliated with the Iranian government is a heinous tactic aimed at silencing the voices of opposition, human rights defenders, and opponents of

[41] محاولة اغتيال المدافعة عن حقوق الإنسان لودي ريمون ألبرتي، فرونت لاين ديندير ، أغسطس 2020 ، https://bit.ly/3wqPvK9
[42] الجيوش الإلكترونية في العراق آلاف الحسابات الوهمية وأسماء بنات لهدف واحد، الحرة ، يناير 2021 ، https://arbne.ws/3DB5W9N
[43] الجيوش الألكترونية حيوانات رقمية مفترسة والأسوأ في الشرق الأوسط، الشرق ، يونيو 2021 ، https://bit.ly/3iZC9zI
[44] إعلاميون من أجل الحرية تدين التعرّض لليال الاختيار، المركزية ، يناير 2021 ، https://bit.ly/2Pv6jj0

the human rights violations in which the Iranian government is implicated and its illegal interference in many countries' affairs in the Middle East.

Recommendations

In sum, modern technologies and applications pose an imminent threat to the basic principles of democracy; they undermine and restrict individual freedoms and put civil society organizations and political opposition in a state of self-censorship for fear of being punished while questioning the integrity of electoral processes around the world and trying to delegitimize them. In addition to perpetuating prejudices in the field of criminal justice, as well as limiting the political participation of citizens at all levels. Artificial intelligence applications, cyber-espionage software, and techniques used in cyber-attacks and social media are the most important of these technologies. For this reason, **Maat for Peace, Development and Human Rights** recommends the following:-

- **To the Office of the High Commissioner for Human Rights**: The necessity of developing a strong and binding legal framework for governments and technology companies to avoid the implications of modern technological applications on the principles of democracy.
- **To the governments of countries**: it is necessary to stop using digital technologies that violate the individual freedoms of citizens while not resorting to electronic attacks to undermine confidence in elections, in addition to providing various guarantees for civil society organizations and political opposition to protect them from the danger of cyber-attacks and disinformation campaigns.
- **To the governments of countries**: the need to cooperate to protect themselves from electronic attacks, in addition to technical cooperation with cyber security companies to secure the information infrastructure of countries, and taking action against governments that use electronic attacks to achieve their goals.
- **To state governments**: the necessity of establishing a human-based unit to monitor artificial intelligence systems working in the field of criminal justice to ensure the rule of law.
- **To human rights activists and political opposition figures affected by new digital technologies**: the need to prosecute notorious technology companies -

which sell applications and malicious software to repressive governments - in many countries of the world in preparation for imposing sanctions on them.

- **To civil society organizations**: the need to install protection software on the devices of human rights activists and opposition figures to secure their accounts, and to discover whether their accounts were hacked by governments or companies through spying tools, such as the Detekt software, which is a simple computerized tool that notifies activists to the presence of hacks in their accounts. CSOs must also work to establish many platforms that correct false information on social media.
- **To technology companies involved in selling digital tools and technologies to repressive governments**: it is necessary to pledge to implement transparent, serious, and rapid investigations into the sale of digital tools and technologies to repressive countries and to oversight them to prevent the sale of products to clients proven to have violated peoples' rights, to ensure that they are not again involved in human rights violations.