PALAIS DES NATIONS • 1211 GENEVA 10, SWITZERLAND
www.ohchr.org • TEL: +41 22 917 9000 • FAX: +41 22 917 9008 • E-MAIL: registry@ohchr.org

Mandate of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression

---

Research Paper 1/2019
June 2019
Freedom of Expression and Elections in the Digital Age

Contents

I. Introduction

This report examines the international standards and principles applicable to the protection of freedom of opinion and expression during elections in the digital age. In his 2014 report to the Human Rights Council, the previous mandate holder examined the State's obligations to respect and ensure freedom of expression in electoral contexts.[1] This report reviews the nature and scope of these obligations in light of advances in technology and their impact on elections.

Advances in information and communications technology have been critical to facilitating access to information and the free flow of ideas during elections. However, State and non-State actors have also exploited these advances to interfere with democratic participation and access to information during election periods, and to undermine the integrity of electoral processes. This report will focus on four such interferences: network shutdowns, efforts to combat the perceived spread of "fake news" and online disinformation, Direct Denial of Service ("DDoS") attacks and interference with voters' records and data.

II. Freedom of Expression and Elections

A. General Legal Framework

The right to freedom of opinion and expression is a "central pillar of democratic societies, and a guarantor of free and fair electoral processes, and meaningful and representative public and political discourse".[2] Article 19(1) of the International Covenant on Civil and Political Rights ("ICCPR") protects the right of "everyone" to "hold opinions without interference". Article 19(2) further establishes the right to freedom of expression, which encompasses the "freedom to seek, receive and impart information and ideas of all kinds". The Human Rights Council and General Assembly have stated that the rights individuals enjoy offline also apply online.[3]

As the language of Article 19(1) indicates, the right to freedom of opinion is absolute. Restrictions on freedom of expression are permissible only if they comply strictly with the criteria established under Article 19(3). Under Article 19(3), any restriction must be "provided by law and necessary" to protect "the rights or reputations of others" and "for the protection of national security or of public order, or of public health or morals". Under the requirement of legality, restrictions must not simply be formally enacted as law; they should also "be made accessible to the

[1] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, Human Rights Council, U.N. Doc. A/HRC/26/30 (Jul 2, 2014), *available at* http://undocs.org/A/HRC/26/30.
[2] *Id.*, at 10.
[3] H.R.C. Res. 26/13, The Promotion, Protection and Enjoyment of Human Rights on the Internet (July 14, 2014), *available at* https://undocs.org/en/A/HRC/RES/26/13; H.R.C. Res. 32/13, The Promotion, Protection and Enjoyment of Human Rights on the Internet (June 27, 2016), *available at* https://undocs.org/en/A/HRC/RES/32/13; G.A. Res. 68/167, The Right to Privacy in a Digital Age, at 1 (Dec. 18, 2013), *available at* http://undocs.org/A/RES/68/167.

public" and "formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly".[4] Furthermore, restrictions must not confer unfettered discretion on those charged with their execution.[5]

Under the requirement of necessity, restrictions must be proportionate to achieve a legitimate government objective. In particular, restrictions must "target a specific objective and not unduly intrude upon the rights of targeted persons", and must be "the least intrusive instrument among those which might achieve the desired result".[6]

Article 25 of the ICCPR protects the right of every citizen to "take part in the conduct of public affairs, directly or through freely chosen representatives", and to "vote and ... be elected at genuine periodic elections which shall be held by secret ballot, guaranteeing the free expression of the will of the electors". Articles 25 and 19 are closely interlinked. The Human Rights Committee has observed that citizens "take part in the conduct of public affairs by exerting influence through public debate and dialogue with their representatives".[7] This participation "is supported by ensuring freedom of expression, assembly and association".[8] Voters should be "free to support or oppose their government" and "should be able to form opinions independently, free of violence or threat of violence, compulsion, inducement or manipulative interference of any kind".[9] Similar to limitations on Article 19, restrictions on Article 25 must be based on objective and reasonable criteria".[10]

The right to privacy also has significant implications for the exercise of freedom of expression in electoral contexts. Article 17 of the ICCPR protects the individual against "arbitrary or unlawful interference with his or her privacy, family, home or correspondence" and provides that "everyone has the right to the protection of the law against such interference or attacks".

This linkage is increasingly evident in the digital age, as personal data of citizens who are eligible to vote has become more susceptible to mass surveillance and digital interception. The General Assembly, the United Nations High Commissioner for Human Rights and special procedure mandate holders have all recognized that privacy is a precondition to the exercise of other human rights,

---

[4] U.N. Human Rights Comm., General Comment No. 34, Article 19, Freedoms of Opinion and Expression, U.N. Doc. CCPR/C/GC/34 (Sept. 12, 2011), at ¶ 25, *available at* http://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf.

[5] *Id.*

[6] *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye*, Human Rights Council, U.N. Doc. A/HRC/29/32 at ¶ 35 (May 22, 2015), *available at* https://freedex.org/wp-content/blogs.dir/2015/files/2015/10/Dkaye_encryption_annual_report.pdf; *see also id.*, at ¶ 34.

[7] U.N. Human Rights Comm., General Comment No. 25 (57), U.N. Doc. CCPR/C/2/Rev.1/Add.7 (Aug 27, 1996) at ¶ 8, *available at* http://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2fPPRiCAqhKb7yhsjYoiCfMKoIRv2FVaVzRkMjTnjRO%2bfud3cPVrcM9YR0iue72QY8oFMq1RR28eUM15L6J1AOT2xcs2D4FgEfOt2liQW2PD1ZsA%2b80ZwK8QWtFzkUhNMfDhFSjgtoCvezhWA%3d%3d.

[8] *Id.*

[9] *Id.*, at ¶ 19.

[10] *Id.*, at ¶ 4.

particularly the freedom of opinion and expression.[11] The former High Commissioner has elaborated that interference with the right to privacy has a "potential chilling effect" on other rights, "including those to free expression and association".[12]

Under Article 17, States should establish legislation that prohibits unlawful and arbitrary interference and attacks on privacy, whether committed by government or non-governmental actors. Such protection must include the right to an effective remedy for violations of privacy.

B. Standards for the Protection of Freedom of Opinion and Expression During Elections

In 2014, the Special Rapporteur outlined the "pillars of an equitable legal framework that would ensure the protection of the freedom of opinion and expression during electoral processes".[13] This section summarizes these principles and standards.

1. Pluralism and the Media

States should encourage an ideologically pluralistic political process. A pluralistic political process is a "regulatory environment that facilitates a diverse range of political positions and ensures that voters have access to comprehensive, accurate and reliable information about all aspects of the electoral process".[14] The media plays a critical role in promoting pluralism, "framing electoral issues, informing the electorate about the main developments, and communicating the platforms, policies and promises of parties and candidates".[15]

Nondiscriminatory access to media should also be guaranteed to all political parties and candidates in compliance with Article 2(1) of the ICCPR, which guarantees the rights established in the Covenant "without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status". Restrictions imposed on media access should also comply with the requirements of legality, necessity and proportionality under Article 19(3). Overbroad or ambiguous regulations tend to encourage discrimination in their enforcement.

Beyond providing equal access to the media, States should encourage a fair system of paid political advertising and allow parties to generate funds to afford doing so.[16] Access to the media is selective if powerful financial parties obtain a competitive

---

[11] *See* G.A. Res. 68/167, *supra* n. 3; HRC. Res. 32/13, *supra* n. 3; U.N. High Commissioner for Human Rights, The Right to Privacy in the Digital Age, U.N. Doc. A/HRC/27/37 (June 30, 2014), *available at* https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf.

[12] *Id.*, A/HRC/27/37 at ¶ 20.

[13] A/HRC/26/30, *supra* n. 1 at ¶ 46.

[14] *Id.*

[15] International Mechanisms for Promoting Freedom of Expression, *Joint Statement on the Media and Elections* (2009), *available at* https://www.osce.org/fom/37188?download=true.

[16] A/HRC/26/30, *supra* n. 1 at ¶ 14.

advantage in marketing. States should seek a balanced approach when addressing this obstacle. Poorly regulated campaign finance laws allow certain individuals to exert undue influence on political candidates and parties. On the other hand, overly regulated campaign finance laws may impede full and free participation in political and electoral processes by limiting the way a party may disburse their funds.

Finally, to promote pluralism, States should ensure that the media is free, independent and diverse.[17] The Human Rights Committee has observed that "undue media dominance or concentration by privately controlled media groups", may be "harmful to the diversity of sources and views" in public discourse.[18] Accordingly, the State's duty to protect the diversity of media sources and prevent "monopolistic situations" is critical to the dissemination of opposing viewpoints during elections and creating a media environment that is conducive to informed decision making.[19] Furthermore, instead of imposing onerous and punitive restrictions that are likely to censor the media, States should encourage and promote robust self-regulatory mechanisms that develop and monitor compliance with ethical standards.[20] When media outlets are State-owned, legal frameworks should be in place to ensure all parties have equal access to the media. Such frameworks should also prevent incumbents from using their position to influence State-owned media in their favor.

2. Transparency

States should strive for transparency in all aspects of the electoral process.[21] One key way to promote freedom of expression is for States to provide meaningful information that allows public scrutiny of the electoral process. For example, disclosure requirements concerning campaign finances are critical to ensuring the fairness and integrity of elections. Information concerning how the integrity of elections is guaranteed (such as processes concerning how ballots are counted and how voting machines are maintained) is critical to ensuring public confidence in free and fair elections. Electoral authorities should also provide meaningful access to ballot counting and results tabulation in order for citizens and parties can verify the accuracy of election results.

States should establish legal frameworks that ensure transparency about media ownership and their potential influence over the political process. As mentioned above, a free and impartial media is critical to public discourse and democratic participation during elections. Relevant disclosures about media ownership and consolidation provide the public with information about possible sources of economic and political influence and bias in the media.[22]

3. Accountability

[17] *Id.*, at ¶ 15.
[18] General Comment 34, *supra* n. 4 at ¶ 40.
[19] *Id.*
[20] *Id.* at ¶ 56.
[21] A/HRC/26/30, *supra* n. 1 at ¶ 61.
[22] A/HRC/26/30, *supra* n. 1 at ¶ 67.

States should have mechanisms in place to monitor, record, address, and provide redress for violations of freedom of expression during the electoral process.[23] In particular, States should create electoral commissions with responsibilities to guarantee elections that meet international obligations and standards such as "election monitoring, the regulation of political funding, the provision of direct access to public broadcasting media and the monitoring of political speech".[24] Upon creating electoral commissions, States should devote the resources necessary for the commissions to operate effectively.

Opinion polls are also another effective tool for holding politicians accountable.[25] However, opinion polls can also be manipulated to influence electoral processes "on the basis of the opinions of a small and non-representative segment of society".[26] Thus, States should ensure transparency by requiring the disclosure of methodologies used in polling to prevent the spread of misleading information derived from non-representative sample groups.[27]

Another component of electoral accountability is to provide redress for violations of human rights during elections. Under Article 2(3)(a) of the ICCPR, States are obliged to ensure that "any person whose rights or freedoms are violated … have an effective remedy". Under Article 2(3)(b), claims of rights violations must be "determined by competent judicial, administrative or legislative authorities, or by any other competent authority provided for by the legal system of the State". The Committee emphasizes the need for administrative mechanisms such as law enforcement and the prosecution to "investigate allegations of violations promptly, thoroughly and effectively through independent and impartial bodies".[28] In the context of elections, harassment and violence against reporters or political candidates should be prohibited by law, and promptly investigated by the relevant authorities.

III. Challenges to Elections in the Digital Age

In recent years, States and non-state actors have increasingly used the digital space to threaten freedom of expression during elections. These threats include, but are not limited to, network disruptions, anti-"fake news" initiatives, Direct Denial of Service ("DDoS") attacks, and interferences with voters' records and data.

A. Network Shutdowns

A growing number of States are intentionally disrupting internet and telecommunications access during election periods.[29] Network shutdowns are

[23] A/HRC/26/30, *supra* n. 1 at ¶ 69.
[24] A/HRC/26/30, *supra* n. 1, at ¶ 71.
[25] A/HRC/26/30, *supra* n. 1, at ¶ 19.
[26] A/HRC/26/30, *supra* n. 1, at ¶ 72.
[27] A/HRC/26/30, *supra* n. 1, at ¶ 72.
[28] General Comment No. 31 [80], The Nature of the General Legal Obligation Imposed on States Parties to the Covenant, U.N. Doc. CCPR/C/21/Rev.1/Add.13 (May 26, 2004), at ¶ 15.
[29] See e.g. Special Rapporteurs' Communications UA TGO 1/2017, *available* at https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=23362; AL CMR 2/2017, *available at*

disruptions that "involve measures to intentionally prevent or disrupt access to or dissemination of information online in violation of human rights law".[30] In 2017 alone, there were at least 108 documented shutdowns.[31]

Network shutdowns are fundamentally incompatible with Article 19(3) of the ICCPR. The Human Rights Committee has stated that "generic bans" on the operation of "websites, blogs or any other internet-based, electronic or other such information dissemination system, including systems to support such communication, such as internet service providers or search engines", are not compatible with Article 19(3).[32] In their 2011 Joint Declaration on freedom of expression and the Internet, independent monitors of freedom of expression and the media in the UN, the Americas, Europe and Africa concluded that "[c]utting off access to the Internet, or parts of the Internet, for whole populations or segments of the public (shutting down the Internet) can never be justified, including on public order or national security grounds".[33] In 2016, the Human Rights Council reaffirmed this basic principle of human rights law, "unequivocally" condemning "measures to intentionally prevent or disrupt access to or dissemination of information online".[34]

Shutdowns may occur in a variety of ways. In addition to network outages, governments may also throttle access to mobile communications, messaging platforms, social media and other websites, rendering them effectively unusable.[35] During election periods, such disruptions inhibit the transmission and receipt of information about candidates and their policies. This implicates the right of voters to know who and what they are voting for, and the right of candidates and political groups to communicate with voters. Shutdowns also prevent voters from accessing critical and time-sensitive updates regarding their polling places and other election day information. Finally, shutdowns may also undermine the individual's ability to

---

https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=22974; AL GMB 1/2017, *available at* https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=22941; AL TCD 3/2016, *available at* https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=22826; ARTICLE 19, *Uganda: Blanket ban on social media on election day is disproportionate*, article19.org (Feb 18, 2016), *available at* https://www.article19.org/resources/uganda-blanket-ban-on-social-media-on-election-day-is-disproportionate/; Filip Stojanovski, *WhatsApp and Viber blocked on election day in Montenegro*, Global Voices (Oct 17, 2016), *available at* https://advox.globalvoices.org/2016/10/17/whatsapp-and-viber-blocked-on-election-day-in-montenegro/.

[30] *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, Human Rights Council, U.N. Doc. A/HRC/35/22 (Mar 30, 2017), at ¶ 8 *available at* https://docs.google.com/viewerng/viewer?url=http://freedex.org/wp-content/blogs.dir/2015/files/2017/05/AHRC3522.pdf&hl=en.

[31] https://www.accessnow.org/keepiton/

[32] General Comment 34, *supra* n. 4 at ¶ 43.

[33] International Mechanisms for Promoting Freedom of Expression, *Joint Declaration on Freedom of Expression and the Internet* (2011), *available at* https://www.osce.org/fom/78309?download=true.

[34] HRC. Res. 32/13, *supra* n. 3.

[35] A/HRC/35/22, *supra* n. 30 at ¶ 8.

exchange information about and engage in political activities, such as rallies, demonstrations and protests.

Given that there is frequently no legal basis for such disruptions, shutdowns violate the Article 19(3) requirement that restrictions on freedom of expression must be "provided by law". In 2016, the Special Rapporteur conveyed concerns about the lack of meaningful public explanation concerning prolonged disruptions to the Internet and social media in Chad.[36] Similarly, Gabon shut down the Internet despite repeated assurances that it would not restrict Internet and telecommunications access.[37]

Even when shutdowns are legally authorized, they violate the requirements of necessity and proportionality. In Pakistan, the High Court of Islamabad held that a policy directive authorizing the shutdown of telecommunications services because of "national concerns" was an overbroad and unlawful assertion of executive power.[38] Ambiguous laws that permit broad government discretion to shut down or otherwise disrupt Internet and telecommunications access have also been documented in Tajikistan, India and the United States.[39]

B. Initiatives to Combat "Fake News" and Disinformation

Following recent contentious electoral seasons, a growing number of States have explored the need for laws and regulations to address the proliferation of disinformation (sometimes referred to as "false" or "fake news") and propaganda during elections. The European Commission's High Level Group of Experts on Fake News and Online Disinformation (the "HLEG") has defined disinformation as "false, inaccurate, or misleading information designed, presented and promoted to intentionally cause public harm or for profit".[40]

In the 2017 Joint Declaration on Freedom of Expression and "Fake News", Disinformation and Propaganda ("2017 Joint Declaration"), the Special Rapporteur together with the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media and other inter-governmental experts, concluded that "general prohibitions on the dissemination of information based on

---

[36] AL TCD 3/2016, *supra* n. 29.
[37] AL GAB 1/2016, *available at* https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=3342 .
[38] *CM Pak Limited vs. The Pakistan Telecommunication Authority*, Islamabad High Court, FAO No. 42 of 2016, *available at* http://mis.ihc.gov.pk/attachments/judgements/F.A.O.%2042-2016%20Against%20Order%20-finalFAONo.42of2016.CMPakLimitedv.ThePTA,etc.636552442049031490.pdf. Note that the court order has been stayed pending appeal. *See also* Berhan Taye, *An internet shutdown during Pakistan's elections? Not on our watch*, Access Now (July 23, 2018), *available at* https://www.accessnow.org/an-internet-shutdown-during-pakistans-elections-not-on-our-watch/.
[39] A/HRC/35/22, *supra* n. 30 at ¶ 10.
[40] European Commission, *A multi-dimensional approach to disinformation: Report of the Independent High level Group on fake news and online disinformation* (Mar 12, 2018) at 3, *available at* https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation.

vague and ambiguous ideas, including 'false news' or 'non-objective information'" are incompatible with human rights law and should be abolished.[41] They also stressed that the "human right to impart information and ideas is not limited to "correct" statements", and "protects information and ideas that may shock, offend, and disturb".[42]

Despite the uncertainty regarding their reach and impact, disinformation and propaganda may mislead populations and interfere with the public's right to know, particularly during elections. However, governments are also capitalizing on the phenomenon of disinformation to propose and enact laws and regulations that interfere with the freedom of expression by restricting legitimate speech, especially during elections.

In light of the principles set out in the 2017 Joint Declaration, the Special Rapporteur is concerned with recent legislative and regulatory initiatives to restrict "fake news" and disinformation. The Special Rapporteur highlighted many of these concerns in communications sent to Italy,[43] Malaysia[44] and France.[45]

These measures typically contain ambiguous definitions of what constitutes "fake news" or disinformation. As noted in the Special Rapporteur's communication to Italy, vague and highly subjective terms—such as "unfounded", "biased", "false", and "fake"—do not adequately describe the content that is prohibited.[46] As a result, they provide the authorities with broad remit to censor the expression of unpopular, controversial or minority opinions, as well as criticism of the government and politicians in the media and during electoral campaigns. Such ambiguity may also incentivize self-censorship due to fears of prosecution and other penalties. Vague prohibitions of disinformation effectively empower government officials with the ability to determine the truthfulness or falsity of content in the public and political domain, in conflict with the requirements of necessity and proportionality under

---

[41] International Mechanisms for Promoting Freedom of Expression, *Joint Declaration on Freedom of Expression and "Fake News," Disinformation and Propaganda* (Mar 3, 2017) at ¶ 2(a), *available at* https://www.osce.org/fom/302796?download=true.
[42] *Id.*
[43] OL ITA 1/2018, *available at* https://www.ohchr.org/Documents/Issues/Opinion/Legislation/OL-ITA-1-2018.pdf. The Italian Government reiterated its commitment to protect fundamental rights, including the freedom of opinion and expression, in a May 2018 response to the Special Rapporteur's communication on the "Red Button Protocol". The Government's letter confirmed that the protocol was no longer operational as it was conceived solely for the electoral period. OL ITA 1/2018 (Govt.'s Response), *available at* http://www.ohchr.org/Documents/Issues/Opinion/Legislation/ItalyReplyMay2018.pdf.
[44] OL MYS 1/2018, *available at* https://www.ohchr.org/Documents/Issues/Opinion/Legislation/OL_MYS_03.04.18.pdf. In its 11 June 2018 response to the Special Rapporteur's communication on the Anti-Fake News Act 2018, the Government stated that it is in the process of repealing the law. OL MYA 1/2018 (Govt.'s Response), *available at* https://www.ohchr.org/Documents/Issues/Opinion/Legislation/ReplyMalaysiaOL.pdf
[45] OL FRA/5/2018, *available at* https://www.ohchr.org/Documents/Issues/Opinion/Legislation/OL-FRA-5-2018.pdf. The government responded on 26 July 2018: OL FRA/5/2018 (Govt.'s Response), *available at* https://www.ohchr.org/Documents/Issues/Opinion/Legislation/ResponseFrance26Jul2018.pdf.
[46] OL ITA 1/2018, *supra* n. 43.

Article 19(3). These restrictions also run contrary to Article 25's requirement that restrictions be based on objective and reasonable criteria.

The imposition of criminal sanctions and other penalties exacerbates these concerns. Malaysia's Anti-Fake News Act of 2018 makes it an offense for "anyone who knowingly creates, offers, publishes, prints, distributes, circulates or disseminates any fake news or publication containing fake news".[47] This offense is punishable with a fine of up to 500,000 Malaysian Ringgit, six years' imprisonment or both. Legislation that would repeal the Act has stalled in the upper house of Parliament,[48] and it remains a paradigmatic example of the type of criminalization that is unnecessary and disproportionate under Article 19(3).

The Human Rights Committee has observed, in the context of defamation laws, that "the application of the criminal law should only be countenanced in the most serious of cases and imprisonment is never an appropriate penalty".[49] A similar presumption against the criminalization of expression also applies to restrictions on "fake news" and disinformation. Laws that impose heightened penalties for persons found guilty of spreading "fake news" or defaming public officials are of particular concern during elections, as they inhibit the right to information about candidates, their platforms and ongoing public debate. Access to such information is critical to the promotion of free and fair democratic elections. Without this information, state actors can manipulate public debate and undermine electoral processes.

Laws and regulations that require (or pressure) private entities to censor or remove content based on vague and ambiguous criteria are also a threat to the exercise of free expression.[50] Private entities are ill-equipped to monitor and regulate such content, and the possibility of facing punitive sanctions or the loss of the ability to operate can force platforms to over-regulate and disproportionately censor a wide range of permissible content.[51] Moreover, these requirements would be particularly burdensome during electoral periods, as platforms would be hard-pressed to meet their duties to monitor and remove content during periods of heightened political discourse and debate. While there is increasing pressure to automate the detection and removal of offending content, AI-based content moderation systems are still limited in their ability to assess "context and take into account widespread variation of language cues, meaning and linguistic and cultural particularities."[52]

---

[47] OL MYS 1/2018, *supra* n. 44.
[48] Hashini Kavishtri Kannan and Ahmad, *PM: Malaysia will repeal Anti-Fake News Act*, New Straits Times (Apr 9, 2019), *available at* https://www.nst.com.my/news/nation/2019/04/477778/pm-malaysia-will-repeal-anti-fake-news-act.
[49] General Comment 34, *supra* n. 4 at ¶ 47.
[50] *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, Human Rights Council, U.N. Doc. A/HRC/38/35 (Apr 6, 2018) at ¶¶ 15 - 17, *available at* https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/096/72/PDF/G1809672.pdf?OpenElement.
[51] *See* OL OTH 41/2018, *available at* https://www.ohchr.org/Documents/Issues/Opinion/Legislation/OL-OTH-41-2018.pdf.
[52] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, General Assembly, U.N. Doc. A/73/348 at ¶ 15 (August 29, 2018), available at https://documents-dds-ny.un.org/doc/UNDOC/GEN/N18/270/42/pdf/N1827042.pdf?OpenElement.

Furthermore, these systems may be trained on "datasets that incorporate discriminatory assumptions" and "make it difficult to scrutinize the logic behind content actions."[53] These factors, coupled with a regulatory environment that incentivizes over-moderation, are likely to generate excessive censorship during electoral periods.

Less intrusive means of addressing the spread of online disinformation are available to both States and companies. Accordingly, approaches for combating disinformation should be evidence-based and tailored to proven or documented impacts of disinformation and propaganda. Rather than imposing undue restrictions on freedom of expression and onerous intermediary liability obligations, efforts to address online disinformation should promote an enabling environment for freedom of expression. These measures include: requiring or encouraging heightened transparency regarding advertisement placements and sponsored content;[54] developing and promoting independent fact-checking mechanisms;[55] providing support for independent and diverse public service media outlets;[56] instituting measures to improve public education and media literacy;[57] and collaborating with social media platforms to ensure that their approaches to content moderation, including the use artificial intelligence-driven tools, reinforce and respect human rights.[58]

C. DDoS Attacks

During elections, State actors have historically denied access to unfavorable views and information concerning incumbent office holders.[59] In the digital age, technological advances have enabled perpetrators to increase the scope and frequency of these attacks on freedom of expression. One common practice involves the use of Distributed Denial of Service ("DDoS") attacks, where a network of online systems is compromised and directed to flood another online system with Internet traffic, effectively rendering the target inaccessible. These attacks have targeted the websites of political parties,[60] journalists and media

---

[53] *Id.*, at ¶¶ 15 – 16.
[54] See e.g. Lawrence Norden, Ian Vandewalker, *This Bill Would Help Stop Russia From Buying Online Election Ads*, Brennan Center for Justice (Oct 19, 2017), *available* at https://www.brennancenter.org/blog/bill-would-help-stop-russia-buying-online-election-ads; *see also* 2017 Joint Declaration, *supra* n. 41 at ¶ 4(b).
[55] 2017 Joint Declaration, *supra* n. 41 at ¶ 4(e).
[56] *Id.*, at ¶ 3(c).
[57] *Id.*, at ¶ 3(e).
[58]
[59] *See e.g.* AL KEN 3/2018, *available at* https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=23632; UA UGA 3/2016, *available at* https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=3162; UA KHM 3/2016, *available at* https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=19826.
[60] Daina Beth Solomon, *Cyber attack on Mexico campaign site triggers election nerves*, Reuters (Jun 13, 2018), *available at* https://www.reuters.com/article/us-mexico-election-cyber/cyber-attack-on-mexico-campaign-site-triggers-election-nerves-idUSKBN1J93BU.

outlets,[61] and human rights defenders and civil society organizations.[62] Perpetrators have also targeted the websites of States' election commissions, which publicize critical information such as changes to ballot locations.[63] DDoS attacks are also potentially a cover for coordinate hacks on voter registration and other electoral databases and other attempts to steal the data of voters, candidates and public officials.[64] Given that online media have become the primary resource of news and information for many voters, and the integration of electronic systems into electoral processes, DDoS attacks are likely to increase in magnitude and frequency. Furthermore, in the Internet of Things era, the growing number of connected devices makes them attractive targets for DDoS attacks.

These attacks, whether committed by State actors or their agents, are incompatible with Article 19 of the ICCPR. Given their covert and illicit nature, these attacks usually violate the requirement that restrictions on freedom of expression must be "provided by law". Such attacks also disable access to entire blogs, websites or electronic systems for the dissemination of time-sensitive and critical information during the election period. Accordingly, they are almost always unnecessary and disproportionate measures under Article 19(3).

When DDoS attacks have been committed by foreign States or non-State actors, States have an obligation to conduct appropriate investigations and provide effective remedies under Article 2 of the ICCPR. Such measures may include the investigation and public release of log files of IP addresses connected to the attack, and tracking the source of malware responsible for the attack.

Because DDoS attacks function by way of flooding an internet server, companies that control online usage and server traffic play important roles in curbing these attacks. Under the UN Guiding Principles on Business and Human Rights, "the responsibility to respect human rights requires that business enterprises . . . seek to prevent or mitigate adverse human rights impacts that are directly linked to their operations, products or services by their business relationships, even if they have not contributed to those impacts".[65] As part of their responsibility to respect freedom of expression, companies should invest resources in security measures and

---

[61] *DDoS used to disrupt elections,* Network Security Newsletter (Dec 2011), *available at* https://www.sciencedirect.com/science/article/pii/S1353485811701234 (stating that "many popular media sites, including those belonging to radio station Ekho Moskvy (Moscow Echo) and news portal Slon.ru" came under a "coordinated DDoS attack" during the 2011 elections in Russia).

[62] *See e.g. Cyber attacks increasing against civil society in Azerbaijan ahead of election*, Access Now (Feb 9, 2018), *available at* https://www.accessnow.org/cyber-attacks-increasing-civil-society-azerbaijan-ahead-election/.

[63] *See e.g.* Taylor Hatmaker, *A cyberattack knocked a Tennessee county's election website offline during voting*, TechCrunch (May 4, 2018), *available at* https://techcrunch.com/2018/05/04/tennessee-election-ddos-knox-county-voting/.

[64] Kim Zetter, *Hacker Lexicon: What Are DoS and DDoS Attacks?,* Wired (Jan 16, 2016), *available at* https://www.wired.com/2016/01/hacker-lexicon-what-are-dos-and-ddos-attacks/.

[65] United Nations, *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect, and Remedy Framework* (2011), at Principle 13(b), available at http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf.

improvements to infrastructure that prevent or mitigate the effects of DDoS attacks involving their products or services.[66]

D. Interference with Voter Records and Voters' Data

Interferences with electoral databases and voters' data are also critical threats to the integrity of elections. Voter records maintained by government authorities, such as voter registration databases, are particularly susceptible to hacking and other malicious attacks.[67] The lack of adequate security protocols and safeguards may also lead to inadvertent exposures of private and confidential voter information.[68] Whether deliberate or inadvertent, such data breaches not only interfere with the right to privacy but also the rights to freedom of expression and genuine democratic elections. As a result, they engage the State's obligations to conduct appropriate investigations and provide effective remedies.

Interferences with personal data held by social media and other Internet platforms may facilitate efforts to covertly manipulate or influence voters. Recent reporting indicates that a researcher obtained access to the personal data of millions of Facebook users through a third party app he had created on Facebook, and shared the data obtained with data analysis firm Cambridge Analytica.[69] Such data was reportedly used to identify and profile voters and target them with political messages.[70] These events demonstrate the close relationship between the privacy of users' data and the exercise of freedom of expression and the right to vote during elections. Companies that hold large amounts of users' data should develop robust and meaningfully transparent privacy policies and processes in consultation with civil society and other stakeholders, consistent with their responsibilities to respect human rights.

IV. Conclusion

Threats to elections in the digital age are complex and multi-faceted, and implicate a wide range of State and non-State actors. Network shutdowns stifle access to

---

[66] *See e.g.* Lily Hay Newman, *Jigsaw's Project Shield Will Protect Campaigns From Online Attacks*, Wired (May 16, 2018), *available at* https://www.wired.com/story/jigsaw-protect-campaigns-from-online-attacks/.

[67] Leah Rosenboom, *Transparency Is Solution to Shameful Lack of Security For US Voting Systems Revealed by NSA Leak*, American Civil Liberties Union (Jun 27, 2017), *available at* https://www.aclu.org/blog/privacy-technology/transparency-solution-shameful-lack-security-us-voting-systems-revealed-nsa.

[68] Joseph Lorenzo Hall, *Campaign Data Breaches: Political Toxic Waste*, Center for Democracy and Technology (Jun 27, 2017), *available at* https://cdt.org/blog/campaign-data-breaches-political-toxic-waste/. Lily Hay Newman, *The Scarily Common Screw-Up That Exposed 198 Million Voter Records*, Wired (Jun 19, 2017), *available at* https://www.wired.com/story/voter-records-exposed-database/.

[69] Mark Zuckerberg, Facebook Post (Mar 21, 2018), *available at* https://www.facebook.com/zuck/posts/10104712037900071.

[70] Carole Cadwalladr and Emma Graham-Harrison, *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach*, The Guardian (Mar. 17, 2018), *available at* https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

critical information and public discourse during electoral periods. While the rise of "fake news" has raised concern about their impact on political discourse, censorship-based efforts to counter disinformation also threaten to suppress legitimate expression and compromise genuine democratic processes. The growth of digital attacks, such as DDoS attacks and the hacking of voter records, pose critical threats to individuals and societies as a whole. Thus, as public discourse gradually migrates to private online infrastructure, companies must play an essential role in safeguarding the exercise of freedom of expression, particularly during elections.

Recommendations

Given these developments, the State's obligation to respect and ensure the right to freedom of opinion and expression is more vital than ever. States should refrain from network shutdowns, which are a categorical violation of international human rights law. They must also ensure that any restriction on blogs, websites, online content and communications platforms is provided by law, and a necessary and proportionate means to protect a legitimate objective. Restrictions on the advocacy of democratic values and human rights are never permissible under these standards.

States should devote sufficient resources and engage relevant expertise (including human rights and civil society expertise) to conduct independent studies into the spread of online disinformation and their impact on elections and political discourse. States should refrain from general and ambiguous prohibitions on the dissemination of information, such as "falsehoods" or "non-objective information". Any restriction on online content, whether directly imposed on users or through the imposition of intermediary liability, should comply with the requirements of legality, necessity and proportionality. In any event, States should consider less intrusive measures for addressing online disinformation, such as the promotion of independent fact-checking mechanisms and public education campaigns.

States should refrain from digital attacks against election infrastructure, including the hacking of election websites and voter records. States that are targets of digital attacks should ensure that they conduct appropriate investigations and develop laws, policies and mechanisms to ensure effective remedies for violations of the right to freedom of expression. States should also take appropriate preventive measures that protect the integrity and security of election infrastructure.

Companies that provide online communications infrastructure and platforms for digital discourse are central to the exercise of freedom of expression during elections. When faced with demands or requests to shut down or unduly restrict websites, they should seek to prevent or mitigate the adverse human rights impacts of their involvement to the maximum extent allowed by law. In any event, they should take all necessary and lawful measures to ensure that they do not cause, contribute or become complicit in human rights abuses. These include human rights due diligence, rights-oriented design and engineering choices and sustained and meaningful consultations with human rights groups, civil society, local communities and other stakeholders.

Companies should also develop and consistently update their privacy policies, processes and safeguards to prevent third party interference with user data. These should be developed in consultation with civil society, privacy experts, local communities and other stakeholders. In addition to regular transparency reporting, companies should promptly disclose information and findings regarding any breach of or undue interference with users' data.