

Digital Election Observation: Regulatory Challenges around Legal Online Content

BEN WAGNER 

Abstract

Between public debates about ‘hacking’ elections, so-called ‘fake news’ and online disinformation campaigns, it has become hard to imagine what free and fair elections in a digital environment could look like. This challenge is particularly pronounced for election observers who monitor free and fair elections. How should election observers fulfil this task when reliable data in online media campaigns are often not even available to media regulators? The following article provides a brief overview of existing challenges around online content regulation and how these apply to elections and election observation. It then considers where resources for digital electoral observation exist and how most effectively to build on these before, in conclusion, discussing next steps and potential opportunities to develop digital election observation further.

Keywords: election observation, regulation, online content, digital campaigning

Introduction

WHILE ELECTIONS have been taking place in digital online spaces for many decades, questions about which types of online content should be considered problematic around elections are relatively recent. Debates about so-called ‘fake news’, disinformation or misinformation and even the ‘hacking’ of elections have all centred on regulating types of online content. Many of the existing challenges with this debate reappear in the debate about ensuring free and fair elections, in particular the debate on regulating criminally illegal content. However, in a regulatory context where even media regulators struggle to gain access to, and verify, all relevant online content, it is not clear how election observers are able to carry out their work effectively.

Given the widespread public debate about a ‘growing problem of illegal and harmful interactions and content online’, the challenges associated with elections should not be forgotten.¹ With an increasing proportion of human interactions taking place in digital contexts, many of the existing challenges with online content moderation are brought to the fore.² At the same time, it is entirely

unclear whether the amount of illegal or harmful content is growing, the proportion of social media uptake is growing, or just that public awareness about the phenomenon is growing. Depending on which of these phenomena is growing, vastly different policy responses would be required.

At present, civil society organisations like Who Targets Me—an organisation that builds a transparency database to make the targeting of individuals by online platforms easier to follow—or the investigative journalists that uncovered the Cambridge Analytica scandal about online targeting during the UK general election, are providing a service to the public without access to sufficient relevant data. It is unacceptable for public institutions to continue in the state they currently are, leaving critical decisions about democratic elections and their governance to private sector online platforms. What might be the consequences for the disinformation and misinformation campaigns that remain unknown to regulators, journalists and the public?

This article provides a brief overview of existing challenges around online content regulation and how these apply to elections and election observation. It then discusses where resources for digital electoral

observation exist and how most effectively to build on these before, in conclusion, discussing next steps and potential opportunities to develop digital election observation further. The empirical scope of the article is limited to election observation and content moderation in Europe.

Regulating illegal *vs* legal content online

Since the earliest days of the internet, there has been a debate about appropriate forms of communication online. However, what was initially a debate about appropriate ways of talking to other human beings quickly evolved to create 'family friendly' spaces, most notably by AOL which was a pioneer of this approach. At the same time, there has been a slew of debates about the appropriateness of regulating different types of content, from spam, trolling, to child sexual abuse material. All forms of content show up on the internet, with some evidently requiring a degree of moderation. Who should conduct this moderation? On which rules it should be conducted and what those rules should look like remains a hotly contested question in a wide variety of different regulatory contexts. Typically, private sector online platforms try to enforce the same norms and standards on their platforms globally. By contrast, national jurisdictions strive to enforce their own legal frameworks onto these platforms, often with limited success.

One of the main challenges in the area of online content regulation is the focus on illegal content, that is, content which is removed from online platforms for legal compliance. One solution proposed in many regulatory debates about online content moderation is that problematic content should be criminalised, and there should be a judicial mechanism to decide about legality. In some cases, content regulatory proposals even go as far as suggesting that all non-illegal content should be required to be kept online. This type of requirement is typically called a must-carry obligation for legal content that creates a right for the restoration of deleted but legal content which has been moderated; a response proposed in debates around the German Network Enforcement Act.

The difficulty with this approach is that it does not consider that the vast majority of content is not removed for reasons of legality or illegality. A World Association of Newspapers and News Publishers (WAN-IFRA) study from 2013 suggests that the average level of content deleted by online platforms is around 11 per cent. An analysis of the content items deleted by an anonymous medium-sized European online platform in the first quarter of 2019 puts this figure at 10.9 per cent, which seems very much in line with the previous estimate from WAN-IFRA. Based on numbers from 2013 and 2019, it seems plausible to argue that the level of deleted content in online forums has remained broadly stable.

Within this 10.9 per cent of deleted content, 4.33 per cent was deleted for reasons of legal compliance, while 95.67 per cent was deleted owing to terms of service violations. In absolute terms, measured against all content on the platform, 0.47 per cent of all platform content is being deleted for legal reasons (based on the platforms' own coding of the reasons for deletion), and 10.43 per cent is deleted for violations of terms of service. The consequences of these figures should be clear: any requirement to reinstate all legal content would reinstate the vast majority of all content currently deleted on online platforms. Online platforms would look significantly different than they do now if all legal content was reinstated. Furthermore, most participants in the debate on online platforms are not aware of the large amount of content currently removed for non-legal reasons. Thus, it seems reasonable to argue that the main challenge online is not in the regulation of illegal content, but rather in ensuring the appropriate governance of terms of service regimes and legal content takedown.

In 2018, the new European Audiovisual Media Services Directive (AVMSD) acknowledged this challenge, establishing a regulatory regime for the terms of service (ToS) of online platforms. In doing so, it shifted the focus of regulation from individual elements of content governed by a public framework and towards the private ordering through elements such as ToS. A similar shift is absent in the German network enforcement law or the European Union's Code of Conduct on the regulation of illegal hate speech, which focusses exclusively on illegal content online.³

This section highlights many of the general challenges associated with online content moderation in general, as well as the specific challenges in focussing on legal or illegal content. Understanding these sets of challenges is important before looking more closely at election related contexts, as they are key to understanding the overall regulatory process relating to online content.

Regulatory challenges around election-related legal online content

So, what should regulators trying to achieve free and fair elections do in this slightly muddled regulatory context? Perhaps the most straightforward option (and most frequently pursued) is simply to make certain forms of online information perceived as problematic illegal, with the posting and hosting of it a criminal offence. While this might seem a straightforward solution, it also poses definitional challenges and creates threats to the very elections it is designed to protect.

Legality of content

Take, for example, disinformation campaigns which have become increasingly abundant online around elections. These campaigns function by spreading factually incorrect information in a strategic manner, thereby shifting the frame of the debate. However, the line between false information and legitimate claims made in the context of a political debate is anything but evident. To provide one example: the renaming of the Facebook account of the UK Conservative Party to 'Fact Check UK' may have been perceived as misleading by voters, but should such behaviour be grounds for criminal liability? To create criminal liability around false political statements would necessarily shift questions of success or failure around political campaigns out of the forum of public debate and into the courtroom.⁴

Legality of funding streams

An alternate strategy would be to restrict and govern the mechanisms by which such

disinformation campaigns can be funded and limit the pool of individuals and organisations able to provide resources to such campaigns. Such restrictions typically relate to geographic limits and individuals who are able to contribute to electoral campaigns. Campaign donations, for example, are not generally allowed from private individuals or corporate actors who are based outside the jurisdiction where the election is taking place: a Swiss corporation or a Spanish citizen is typically prohibited from contributing to political campaigns in Germany. These restrictions also apply to other means of influencing the political process, such as online advertising campaigns. Restrictions of funding are particularly attractive from a regulatory perspective, as they do not require individual decisions about specific pieces of content that run the risk of unduly restricting the political debate around an election. Together with restrictions on sources of funding, it also makes sense to ensure the sources and uses of funding are made as transparent as possible to the electorate.

Transparency requirements

Finally, transparency requirements around pieces of content in the online environment would appear urgently necessary and extremely helpful. The transitory nature of many types of online content, and the closed technical architecture of many more popular online platforms like Facebook or Instagram, make it easy to show widely spread content to specific groups of people without this being available to the general public. This type of electoral content, which has been coined 'dark posts', poses considerable challenges to free and fair elections, as it allows tailoring of different content to different groups of individuals without any accountability for the statements made. Importantly, given the many problems with the accuracy of existing transparency reports provided by online platforms—even if they have a legal basis—an auditing mechanism which ensures the accuracy of all transparency provided is equally important.⁵ This transparency is needed for both popular organic political content, that is, content that is

posted by the users of online platforms, as well as paid advertising content. As a minimum, it is important to know if something is classified as political content, how widespread the most popular political content is, and what type of entity posted it. For paid advertising, information about the amount paid would also be important. If content was removed from the platform, it should also be made clear why this was the case. All of this content should be publicly available globally in a searchable online transparency database. Sadly, this is not currently the case for any large online platform.

This section has discussed some of the main regulatory challenges associated with election related online content and suggests that there is much still to be done if digital election observation is to be a success.

Digital election observation: media monitoring and beyond

Election observation is the process of external monitoring which ensures that democratic elections remain free and fair. It is conducted by an external team of monitors, who look a wide variety of aspects of the electoral process over many months, ranging from the existing electoral laws, to media pluralism, and the fairness of the electoral process on the ground. Typically, election observers are sent by international organisations to monitor elections as either short-term or long-term observers, with the long-term observers beginning their task many months before the election itself. The short-term observers are only involved for a matter of weeks and are focussed primarily on the actual process of the election itself, while the long-term observers assess the overall legal, political, and media context in the specific country.

While election observation remains a crucial element of securing free and fair elections, credible election observation focusses on far more than just voting itself and attempts to take the broader political and media situation into account. For example, the Organization for Security and Co-operation in Europe (OSCE) Office for Democratic Institutions and Human Rights (ODIHR) writes that a 'long-term, comprehensive, consistent and systematic election observation

methodology has become the bedrock of ODIHR's credibility in this field'.⁶ Similarly, the European Commission Election Teams note that 'EU election observation has developed from a short-term, *ad hoc*, operation into a long-term process with a rigorous and systematic methodology'.⁷

Within this long-term approach, media monitoring is a crucial aspect of election observation. Both the OSCE and the EU handbooks on election observation have extensive sections on media monitoring, the role of media supervisory bodies, and a healthy media environment conducive to ensuring free and fair elections. With much of the challenges associated with these topics shifting online, it can be assumed that election observers will need to adapt to new challenges.

As a large part of the electoral debate now takes place online, it could be expected that electoral observation has also moved online. However, this does not seem to be the case. The focus of election observers who conduct media monitoring is currently mainly on print and broadcast media, with very little guidance on how to conduct election observation on social media. Even the latest handbook of the OSCE from 2012, which is explicitly focussed on media monitoring, discusses the internet in general terms, in less than a page, without concrete guidance.⁸

A lack of international standards, conventions, and best practices on how to observe effectively the digital aspects of elections could explain why guidelines for digital election observers are currently lacking. Importantly, the challenges associated with digital election observation are not just related to digital technologies. Instead, these technologies have enabled novel practices that pose challenging in a digital context. These include:

- foreign interference in elections;
- hacking;
- hate speech leading to election-related violence;
- deceptive digital campaign practices;
- insecure digital election equipment and services;
- insufficient political advertising regulations for the online environment;
- a lack of meaningful data about the impact of social media and transparency surrounding political advertising;

- a lack of early warning systems for election-related disinformation, foreign interference, hate crimes, threats to women, violence, and voter suppression.⁹

Importantly, none of these challenges is necessarily a consequence of the increasing use of digital technologies. Instead, the use of new technologies means that existing regulatory frameworks and their institutional support structures need updating. Sadly, this already difficult situation is not helped by a lack of assistance from technology companies. As one leading international election observer noted during the research for this article: 'We're running after the tech companies, they have enormous resources, and they're playing us.'¹⁰

This raises important questions not just about new standards for election observation, but also the specific mechanisms that would be needed for electoral observers and large online platforms to be able to work together. As these mechanisms do not currently exist, there will need to be a process of negotiation from both sides to ensure that an effective relationship can be established. Such a relationship may also the need a specific legal basis and a set of governing rules to support it. Finally, a minimal degree of willingness by private companies to comply is also required. None of these challenges are insurmountable, but require considerable additional work to set standards and build relationships in order to be effective on an everyday basis.

Where are resources for digital election observation needed?

Another fascinating question associated with digital election observation is who should benefit from resources around election observation. At present, the existing technical capacity around election observation is focussed primarily in international organisations such as the European External Action Service (EEAS) of the OSCE ODIHR. While this makes sense organisationally for the typical model of election observation, it can be argued that such technical capacity would also be beneficial for national election authorities and media regulators. These findings are in line with a recent report by the report of the

Kofi Annan Commission, *Elections and Democracy in the Digital Age*, which suggests that:

Some [election monitoring bodies] may find themselves in need of short-term technical assistance against threats to electoral integrity by foreign interference in elections, hacking, and hate speech leading to election-related violence. In such cases, international technical assistance to help [election monitoring bodies] defend their election should be quickly available when requested.¹¹

Were the EU and the OSCE to develop significant technical capacity in the area of digital election observation, such capacity would be in high demand beyond this context. There are two areas where such technical capacity would be particularly valuable: outside current regional areas of scope and outside electoral contexts. For example, existing EU observation capacity would be valuable within the EU, not just outside it. Countries such as Hungary, Austria, Poland or the UK could all benefit from increased EU election observation capacity, as they currently struggle to ensure free and fair digital elections at a national level. The lack of capacity is particularly evident where existing media supervisory bodies struggle with their tasks in the digital sphere. Receiving technical assistance and support through an organisation with higher technical capacity in this area could strengthen the ability of media supervisory bodies to fulfil their tasks effectively. The same can be said for requirements for technical assistance outside electoral contexts, for example, in situations where public trust in existing media supervisory mechanisms has massively deteriorated and the stability of democratic institutions is under threat. In these situations, ensuring free and fair democratic debate in an open environment is crucial to ensuring the voices of citizens are heard and the trust in democratic institutions and media supervision is restored.

Such involvement of digital election observers may raise questions about the impartiality of their work as election observers. It is therefore critical to ensure that any involvement that is organised can only be understood as in support of local technical capacity. At the same time, given that existing local governance structures often struggle to fulfil their existing regulatory tasks in

an online environment, international support may provide a useful mechanism to support free and fair elections.

Conclusion

Digital election observation is a challenge that cuts across existing mechanisms for election observation, media regulation, and democratic governance. The technical capacity and methodological expertise to be able to perform this function should be available to as many parties as possible and not limited to a single set of monolithic international institutions. The more plural and diverse set of actors that have access to technical capacity in this area, the easier it will be to ensure that free and fair elections take place.

Building effective institutions able to respond to the challenges raised by digital media remains a crucial challenge to ensure free and fair elections. The problem is not the phenomenon of disinformation or fake news, but rather a lack of adequate institutional processes that respond effectively to attempts to exploit loopholes in existing campaigning rules via digital means. This article has not primarily tried to suggest that new technologies are changing how elections work, but rather that already weak institutions charged with overseeing democratic elections are overwhelmed by new technologies. Effective institutional responses are neither impossible nor unreasonable; they are primarily a question of political will. Precisely because free and fair elections are so important as a pillar of democratic institutions, it is high time that such political will is forthcoming.

Acknowledgement

Many thanks to Felix Kartte and Sabrina Spieder (European External Action Service), Agustin Rossi and Ben Scott (Luminate), Matthias Vermeulen (Mozilla Foundation), Volker Jacoby (Centre of Excellence for Civilian Crisis Management), Katharine Dommett (University of Sheffield), and Mona Schindler (OSCE), as well as two anonymous reviewers for their valuable input on this article.

Ben Wagner holds a PhD from European University Institute in Florence and his research focusses on technology policy,

human rights, and accountable information systems.

Dr Ben Wagner is an Assistant Professor at the Faculty of Technology, Policy and Management at TU Delft.

Notes

- 1 M. Yar, 'A failure to regulate? The demands and dilemmas of tackling illegal content and behaviour on social media', *International Journal of Cybersecurity Intelligence and Cybercrime*, vol. 1, no. 1, 2018, pp. 5–20.
- 2 B. Wagner, 'The politics of internet filtering: the United Kingdom and Germany in a comparative perspective', *Politics*, vol. 34, no. 1, 2014, pp. 58–71; B. Wagner, 'Freedom of expression on the internet: implications for foreign policy', *Foreign Affairs*, vol. 88, 2011, p. 4.
- 3 N. Alkiviadou, 'Hate speech on social media networks: towards a regulatory framework?', *Information and Communications Technology Law*, vol. 28, no. 1, 2019, pp. 19–35.
- 4 B. Wagner, 'Liable, but not in control? Ensuring meaningful human agency in automated decision-making systems', *Policy and Internet*, vol. 11, no. 1, 2019, pp. 104–122.
- 5 B. Wagner, et al., 'Regulating transparency? Facebook, Twitter and the German Network Enforcement Act', ACM Conference on Fairness Accountability and Transparency, 2020.
- 6 Office for Democratic Institutions and Human Rights, *Election Observation Handbook*, 6th edn., 2010.
- 7 European Commission, *Handbook for European Union Election Observation*, 2nd edn. [rev.], 2008, preface; http://eeas.europa.eu/archives/docs/eucom/pdf/handbook-eucom-en-2nd-edition_en.pdf (accessed 10 August 2020).
- 8 Conference on Security and Cooperation in Europe, *Handbook on Media Monitoring for Election Observation Missions*, OSCE Office for Democratic Institutions and Human Rights, 2012.
- 9 Kofi Annan Foundation, *Protecting Electoral Integrity in the Digital Age*, report of the Kofi Annan Commission on Elections and Democracy in the Digital Age, Kofi Annan Foundation, 2020, pp. 18–22; https://www.kofiannanfoundation.org/app/uploads/2020/01/f035dd8e-kaf_kacedda_report_2019_web.pdf (accessed 11 August 2020).
- 10 Telephone interview with a leading election observer working at an international organisation (speaking in a personal capacity), 12 March 2020.
- 11 Kofi Annan Foundation, *Protecting Electoral Integrity*.