DIGITAL PLATFORMS AND THE DIGITISATION OF GOVERNMENT SURVEILLANCE

Ronan Ó Fathaigh
University of Amsterdam

Rocco Bellanova
University of Amsterdam

Bengi Zeybek
University of Amsterdam

Judith Moeller
University of Amsterdam

In Europe today, digital platforms, such as Facebook, Twitter and YouTube, provide an essential means for millions of people to express themselves, engage in public debate, and organise politically (Poell & van Dijck, 2018). Their crucial role in modern digital societies is increasingly recognised by public institutions. For instance, Europe’s highest human rights court has recently highlighted platforms’ importance for public expression and distribution of news. In the words of the European Court of Human Rights, platforms provide an ‘unprecedented’ means for exercising freedom of expression, ‘undoubtedly’ enhance the public’s access to news, and facilitate the widespread dissemination of information (Cengiz v. Turkey, 2015, para. 52) (see also, Dobber, Ó Fathaigh & Zuiderveen Borgesius, 2019). However, these platforms are built upon vast systems of data collection and data monetization (Cohen, 2017; Ó Fathaigh, Van Hoboken & Van Eijk 2019), which raises major concerns in terms of privacy, data protection and consumer protection. Besides, platforms’ regular use of algorithmic and AI systems is shaping information dissemination, which impacts on users’ freedom of expression (Eskens, Helberger & Möller, 2017).

Crucially, over the past five years in particular, governments have been able to leverage the power of platforms to impose new forms of restrictions on free expression, and engage in the surveillance of individuals and online activism. This has profound

implications for the rights to freedom of expression, privacy, and data protection. Indeed, the UN Special Rapporteur on freedom of expression has highlighted the government ‘pressure’ on digital platforms to implement ‘proactive measures’, including automated tools, that may ‘serve as a form of pre-publication censorship’ (Kaye, 2018, p. 12). Further, platforms that once refused to cooperate with governments in identifying users responsible for disseminating allegedly illegal or harmful content are now expanding cooperation with authorities, including sharing data about users flagged by law enforcement and other authorities. For example, in summer 2019, the French government announced that for the first time, Facebook had agreed to hand over identification data of users suspected of disseminating allegedly illegal content to French judicial authorities (Rosemain, 2019). Other countries, such as the United Kingdom and United States, have announced similar agreements with platforms such as Facebook and Google (Schulze, 2019). While welcomed by public authorities, these forms of platform/government cooperation raise multiple concerns. For instance, civil society organisations note that too many different public authorities seek (and obtain) access to platform users’ data, including not only law enforcement but also intelligence and immigration agencies. As civil society organisations warn, this trend is contributing to ‘invasive and unlawful digital surveillance’ (Amnesty International, 2019 p. 24). As such, platforms are becoming both tools of government and targets for regulation, and taking advantage of regulation by platforms (Gillespie, 2018).

This paper examines how European governments are leveraging the power of digital platforms to engage in government surveillance online, and assesses the compatibility of these measures with European human rights law. The paper applies a unique interdisciplinary perspective, bringing together law, political communication and surveillance studies. Literature on platforms is rapidly burgeoning, especially in the field of law (Ó Fathaigh, Van Hoboken, Van Eijk 2019), media studies and regulation (Gorwa, 2019; Gillespie, 2018; van Dijck, Poell & de Waal, 2018). Yet, interdisciplinary conversations remain rare (Helberger, Pierson & Poell, 2018). First, the paper examines how platforms’ algorithmic systems shape (and limit) information dissemination. The paper then critically analyses government-platform initiatives that exist to surveil citizens and gather information, including new measures under the EU’s proposed Digital Services Act. Third, it assesses how these measures comply with freedom of expression and the right to privacy, and concludes with recommendations on remedying problematic elements of the role platforms play in digitisation of government surveillance.

References


