Article

Online Surveillance in Turkey: Legislation, Technology and Citizen Involvement

Bilge Yesil

College of Staten Island, City University of New York, US.
bilge.yesil@csi.cuny.edu

Efe Kerem Sözeri

Vrije Universiteit Amsterdam, The Netherlands.
eksozeri@hotmail.com

Abstract

The AKP government has constructed an online surveillance regime (not to mention censorship) via various legal and technical means. This article analyzes the emergence and expansion of online surveillance within the context of the AKP's authoritarian practices that are interwoven with its nationalist and populist politics. It begins with an overview of legal and technical initiatives aimed at enhancing online surveillance, data collection and retention. It then focuses on the AKP's recent strategies designed to bolster this online surveillance regime such as the institutionalization of online "snitching" via a newly-introduced social media app that enables citizen-informants to "report terrorists" to the authorities.

The article argues that the AKP's recent strategies and rationalities to regulate the conduct of online users are aligned with principles of "governing at a distance" and are informed by both its authoritarianism (exemplified by the repression of all forms of dissent in the broader media ecosystem) and its right-wing nationalism and populism (as seen in the stigmatizing of critical voices and/or certain groups as sources of threat, labeling them as "being against the nation" and as "terrorists").

Introduction

Since the late 2000s, media and communications in Turkey have been severely restricted. The AKP government (Justice and Development Party) has exerted legal and financial pressure on news media to muzzle critical reporting and tightened the control of the online public sphere as per its nationalist and religious conservative logic (Yesil 2016; Ohm 2015; Akser and Baybars-Hawk 2012; Kurban and Sozeri 2012). At every critical political juncture since 2013, the AKP has amped up its efforts to silence critical journalists, activists, and other politically-engaged actors.¹ In the online sphere, these initiatives have included domain blocking (denying access to an entire IP address), URL blocking (denying access to only certain materials in a given domain), regional internet shutdowns, surveillance and trolling (Telli Aydemir 2016; Saka 2014, 2016; Binark et al. 2015; Freedom House 2016; Yesil et al. 2017).

This article focuses on the construction and expansion of online surveillance, specifically in the post-2013 period. It begins with a brief overview of the AKP's populist and authoritarian politics, and contextualizes

¹ Among the key political developments that took place since 2013 are the nationwide Gezi protests (June 2013), revelations about massive corruption at higher echelons of the government (December 2013), intensified armed conflict in the southeast region of the country (July 2015), and the failed coup attempt (July 2016).

online surveillance as part of a toolkit that seeks to bolster the government's authority in the communicative space. It analyzes administrative, legal, and technical measures that enable collection and storage of user data by state institutions, and the involvement of non-state actors in online surveillance of users.

Populist and right-wing nationalist currents in the post-2013 period

Since coming to power in 2002, the AKP officials emphasized that their mission is to restore power to “the people” and undo the inequalities inflicted by “the elite.” At every local and general election, they deployed this ultimate populist dichotomy of us vs. them, and exploited the cleavages between the socio-economically and politically marginalized populations and the military-secularist establishment.

While right-wing nationalism has always been a hallmark feature of the AKP's political ideology, it has become more pronounced especially in the post-2013 period. Beginning with the Gezi protests and the corruption scandal, the AKP has faced several challenges such as the electoral success of Kurdish candidates in 2015, foreign policy failures and security lapses in 2015-16, and finally the coup attempt in 2016. In response to these legitimacy crises and the status anxiety they generated, the AKP government amplified its existing authoritarian policies and introduced new legislation to impose further restrictions on media and online communications. To legitimize these initiatives, the AKP has instrumentalized a nationalist populist rhetoric that valorizes the good, responsible, and patriotic citizens; included them within the category of “the people” and “the nation” and labeled dissidents and critics as sources of threat.

Specifically, in response to the rise of the Kurdish party in the 2015 elections and the coup attempt that is believed to have been engineered by its former ally Gulen in 2016, the AKP perpetuated an oppositional axis between the so-called good citizens and terrorist others. Notwithstanding the fact that there are certain groups engaged in terrorist activity, the AKP broadened the definition of “terrorist” and “terrorism” to prosecute, arrest, and otherwise silence politicians, journalists, NGO members, academics, and ordinary citizens that dare to criticize its policies on social media. For example, journalists who work for pro-Kurdish outlets and/or report government corruption, foreign policy failures and other sensitive topics have found themselves subject to criminal investigation.² Ordinary citizens also risk prosecution if their social media posts are considered to be spreading terrorist propaganda.³ It is this broader authoritarian and populist political landscape within which the online surveillance regime is constructed, fortified and serves to penalize those who produce and distribute critical news and opinion.

Constructing the online surveillance regime: Legal and technical measures

There is no legislation in Turkey that prohibits online users from posting anonymously. Nor is there a law that requires them to obtain a license or register with government agencies prior to launching websites and blogs. In practice, however, freedom and anonymity of communications is lacking because of the mandatory registration of SIM cards (Privacy International 2014: 6). When purchasing a mobile or smartphone, users in Turkey must submit their national ID number, making it possible for government agencies to “establish extensive databases of user information” and “create comprehensive profiles of individual citizens” (Privacy International 2014: 6).

² Charges against journalists are based on provisions of the Penal Code and Anti-Terrorism Law that criminalize vaguely-defined acts such as “inciting people to hatred and animosity, praising a terrorist organization, disseminating propaganda on behalf of a terrorist organization, and declaring one's affiliation with a terrorist organization.”

³ According to latest available data, 1,656 online users were arrested between December 2016 and May 2017 because of their social media posts, and another ten thousand are currently under criminal investigation (see Birgun Daily 2016).

In addition to this registration scheme, surveillance of online communications is facilitated through a series of legislation concerning internet activity. For example, the Internet Law of 2007 set forth the criteria for blocking websites and governing the activities of ISPs. It obliged the providers to monitor online content transmitted through their infrastructure, and required them to ban access to illegal content upon being served with a court order or an administrative notice.

The first Internet Law (as it is commonly known) was hastily amended by the AKP in February 2014 in response to the so-called damaging effects of digital communications. The increasing use of social media during the nationwide Gezi protests and the online dissemination of critical information about government corruption led the AKP government to introduce stricter provisions concerning content removal and data collection. According to the second Internet Law, ISPs are now required to collect data on users' activities for up to two years and provide authorities with this data on demand. The law pertains to mass use providers including internet cafes and places that provide free WiFi such as universities, coffee shops, restaurants, etc. in the category of access and hosting providers, and thus requires them to obtain activity certificates, implement government's blocking decisions, and store user data (Freedom House 2016).

To facilitate the collection of data, in 2014 the AKP also amended the Law on State Intelligence Services and the National Intelligence Agency. The new legislation enables the intelligence agency—the MIT (known by its Turkish acronym)—to collect personal data, documents and information about individuals without a court order; obtain data from private companies, public authorities, professional organizations and other legal persons; and gain access to data stored in IT devices, equipment and hardware whether they are owned publicly or privately (PEN International 2015: 42; Ozeke 2014).

In another blow to privacy of communications, the AKP amended several laws as part of the Homeland Security Package that was passed in 2015. For example, the new Law on the Powers and Duties of Police allows law enforcement to carry out wiretapping in urgent situations for a forty-eight-hour period without a court order (previously the time limit was 24 hours).⁴ Additionally, in so-called urgent situations the police can request user data from telecommunications companies to locate the user, and monitor and evaluate their communications. Another piece of legislation amended as part of the Homeland Security Package was the Identity Disclosure Law. As per this new legislation, car rental companies and hotels are required to keep daily records of customers' identity and contact information, and “computerize all records and have their computer terminals connected to the computer terminals of law enforcement officials” (Zeldin 2015).

The AKP government's efforts to collect personal data and monitor online communications intensified in 2016 in the aftermath of the botched coup. The AKP government declared a State of Emergency (SoE) for a duration of three months, which it has renewed continuously. Currently in effect, the SoE enables the AKP to legislate through decree laws and without parliamentary approval (European Commission for Democracy through Law 2016: 16).⁵

⁴ The law does not provide a specific definition of “urgent situations.” In this context, however, the term is generally meant to refer to situations whereby there is an imminent danger, a sudden threat or a grave risk to public safety, state sovereignty and national unity. Needless to mention, the intentional use of such vague terms opens the door to various interpretations and possible abuse.

⁵ The SoE and decree laws originally targeted the putschists, but the government has applied these laws to other organizations, groups or individuals considered to be terrorists (e.g. activists, academics, Kurdish politicians and journalists). As result of decree laws, since July 2016 the government has dismissed approximately 100,000 public servants without any investigation or the opportunity of a legal challenge. In addition, it shut down approximately a thousand private companies, charitable organizations, hospitals, private schools and universities, and more than a hundred media outlets (Baglayan 2017).

By June 2017, the AKP government passed twenty-four decree laws, seemingly to “cleanse the army, law enforcement and state institutions from the coup planners and their affiliates; to bring to justice those who are affiliated with terrorist organizations and threaten national security; to restore public order and safety, and to protect democracy and basic rights and freedoms” (European Commission for Democracy through Law 2016: 10) The following section takes a closer look at decree laws that expand the surveillance capabilities of the state.

Decree Law 670 facilitates the interception of digital communications of users who are under a coup-related investigation (as well as their spouses and children) and the collection of their private data from all public authorities and private companies. Decree Law 671 allows the BTK (the government agency that is responsible for regulation of telecommunications sector) to overtake any privately-held digital communications company including cable or cellular network providers to “[maintain] national security and public order; prevent crime; protect public health and public morals; or protect the rights and freedoms [of citizens]” (Sözeri 2016). Last but not least, and in a blow to online privacy, Decree Law 680 enables the Department of Cybercrimes to gather and intercept internet traffic on *any* internet-related investigation and to obtain personal information from ISPs without a court order.

In addition to the legislative measures, there are various technical tools that the authorities use for purposes of online surveillance and data collection. According to research undertaken by Citizen Lab, there is evidence of several digital spyware programs being used in Turkey, although it is not known which government agencies use(d) them, for how long, and if they conduct(ed) targeted surveillance of online users. Among these spyware programs are the following: 1) Phorm, a program that “collects information on users’ online behavior without their knowledge, performs deep-packet inspection (DPI) to monitor a user’s connection line, and creates a profile of the individual’s online activities,” 2) Package Shaper, a program used for internet filtering and surveillance; 3) Remote Control Systems that is produced by the Italian company Hacking Team, and FinFisher that is produced by the UK-German company Gamma International, both of which enable the interception of passwords and emails as well as the remote control of a device’s microphone to record conversations, and 4) Deep Packet Inspection (DPI) technology provided by Procera Networks that Turk Telekom (the largest ISP in Turkey) has used since at least 2014 for mass surveillance of internet traffic (Privacy International 2014: 5-7; Marquis-Boire et al. 2013).

Expanding the online surveillance regime: Recruiting non-state actors

In addition to the above-mentioned legal and technical measures, the AKP government has recently begun to involve non-state actors in the surveillance of online communications in the immediate aftermath of the abortive coup, with the aim of increasing the surveillance capabilities of law enforcement and intelligence agencies. Three days after the coup attempt, the Turkish National Police issued a statement urging citizens to inform law enforcement personnel of social media users that allegedly provoked fear, panic and chaos (Tasdan 2016). Approximately six months after the coup attempt, the Ministry of Interior released a report concerning prosecutions of social media users. According to the Ministry, a total of 3,710 individuals had been prosecuted, with 1,656 arrested, 1,203 released on condition of judicial control, and 767 set free. Charges were specifically about so-called crimes committed via social media such as “inciting public enmity and hatred, propagating on behalf of terrorist organizations, announcing one’s affiliation with terrorist organizations, engaging in defamatory or libelous remarks against state officials, and threatening state sovereignty and public safety” (Iciseri Bakanligi 2016). The Ministry did not specify if or how many of the arrests and detentions were based on information provided by citizens, but a pro-government newspaper announced that the police had received more than seventeen thousand emails concerning social media users who allegedly praised a bombing attack (Simsek and Zengin 2016). The preoccupation with “virtual terrorists” culminated in the launching of a smartphone app and a dedicated webpage by the National Police to enable citizens to report allegedly harmful social media posts. In its public announcements, the National Police urged citizens to share “all available information” concerning users that post “harmful content,” and

advised them to take screen shots in case the said content is deleted. The news of the app was welcomed by pro-government journalists and pundits who wholeheartedly encouraged their fellow citizens to report the alleged “social media terrorists” (Yeni Safak 2016).

In addition to these officially-acknowledged initiatives, there is a purported “Social Media Monitoring Unit” set up by the government.⁶ According to a member of the parliamentary commission on security and intelligence affairs, this group is in the process of preparing legal investigation notices for seventeen thousand users; however, there is no specific information as to which users are selected for surveillance, how they are surveilled, or if their online communications are intercepted (Cumhuriyet 2017).

Conclusion: Online surveillance in an authoritarian regime

The AKP’s efforts to involve ordinary users in online surveillance resonate with the diffusion of surveillance from institutional actors to average citizens, and more specifically with the rise of lateral surveillance (Andrejevic 2005; Chan 2008; Hier and Greenberg 2009; Larsen and Piché 2009). Since the late 20th century, increasing concerns with risk and risk management (Beck 1992; Castel 1991; Ericson and Haggerty 1997; Lyon 2001, 2007) and the attendant logic of self-responsibilization have fueled the rise of lateral surveillance, as seen in community-based programs that aim to prevent neighborhood crime and government campaigns implemented to fight terrorism (Andrejevic 2005: 493). Borne out of concerns with populations that are likely to produce risk, lateral surveillance programs urge citizens to be vigilant, report suspicious persons and activities, and act as the “eyes and ears” of authorities (Chan 2008; Larsen and Piché 2009; Reeves 2012).

In this regard, recent calls made by the AKP and its proxies that encourage social media users to report “virtual terrorists” is an example of lateral surveillance—the state-driven kind. “Thriv[ing] on a culture of social suspicion,” state-driven lateral surveillance initiatives (e.g. the post-September 11 “See Something, Say Something” campaign) aim to mobilize lay citizens to “integrate surveillance into their daily lives,” identify themselves with the “agencies of the state,” and “perform social responsibility as per state objectives like community tranquility or homeland security” (Reeves 2012: 236, 245).

The Turkish National Police’s program that calls on social media users to act as informants is similar to public vigilance campaigns in the sense that they both perform “techniques of policing” and “means of social monitoring and control,” and thus extend the state’s surveillance capacity and power (Larsen and Piché 2009: 188). In this sense, the National Police’s smart phone app aims to overcome the potential limitations and inadequacies of the government’s existing online surveillance regime especially when one considers the near-exhaustion of state resources in investigating and prosecuting huge numbers of social media users.⁷

In the Turkish context, the state-driven lateral surveillance is the latest manifestation of an authoritarian government’s efforts to stifle any remaining opposition in the public sphere. Since the late 2000s, media autonomy in Turkey has declined precipitously as result of prosecution of journalists in politically-motivated investigations and dismissals of critical voices from media organizations by corporate owners.

⁶ The government has neither confirmed nor denied the existence of this unit, and there is no information about the results of its activities.

⁷ While post-September 11 public vigilance campaigns and the AKP’s recruitment of citizens in online surveillance bear certain similarities, their differences must also be noted. Although the lateral surveillance initiatives in the U.S. created a culture of suspicion and had a chilling effect on civil liberties, they were not implemented to institute or bolster an authoritarian regime. In the Turkish case, state-driven lateral surveillance is part of an authoritarian toolkit that aims to silence critics and consolidate hegemony. The authors would like to thank the anonymous reviewer for bringing up this important distinction.

While mainstream and oppositional outlets began to toe the government line out of fear of legal and financial retribution, their pro-AKP counterparts prospered thanks to the generous privatization deals, public tenders and cheap credits they received from the government (Akser and Baybars-Hawk 2012; Finkel 2015). In this increasingly polarized, partisan and clientelistic media system, journalists, activists and dissidents resorted to social media to share news and information, and to express critical views. However, the increasing use of online platforms for purposes of information sharing and political mobilization has brought with it stricter government controls as discussed in previous sections.

Whereas the prosecution of journalists and (the threat of) financial reprisals have led to self-censorship in mainstream news media, online surveillance initiatives now seek to confine the limits of the online public sphere. Targeting not only journalists but also ordinary users, online surveillance establishes norms for permissible speech online, regulates the conduct of users and enables the government to bolster its authority.⁸ The intensification of legal and technical encroachments on digital communications and the recruitment of members of the public in online surveillance must therefore be understood in terms of the AKP's broader agenda to suppress criticism in the communicative space and maintain its legitimacy at all costs.

References

- Akser, M., and B. Baybars-Hawks. 2012. Media and Democracy in Turkey: Toward a Model of Neoliberal Media Autocracy. *Middle East Journal of Culture and Communication* 5 (3): 302-321.
- Andrejevic, M. 2005. The Work of Watching One Another: Lateral Surveillance, Risk, and Governance. *Surveillance & Society* 2(4): 479-497 [Accessed: March 10, 2017].
- Baglayan, B. 2017. The Turkish State of Emergency under Turkish Constitutional Law and International Human Rights Law. *Insights: American Society of International Law* 21 (1). <https://www.asil.org/insights/volume/21/issue/1/turkish-state-emergency-under-turkish-constitutional-law-and> [Accessed March 3, 2017].
- Beck, U. 1992. *Risk Society: Towards a New Modernity*. Sage.
- Binark, M., S. Karatas, T. Comu, E. Koca., 2015. Türkiye'de Twitter'da Trol Kültürü. *Toplum ve Bilim* (135): 124-157.
- Birgun Daily. 2016. 1656 people arrested in Turkey in 6 months for posts on social media. 25 December. <http://www.birgun.net/haber-detay/1656-people-arrested-in-turkey-in-6-months-for-posts-on-social-media-140867.html> [Accessed: March 10, 2017].
- Castel, R. 1991. From Dangerousness to Risk. In: *The Foucault Effect: Studies in Governmentality*, eds G. Burchell, C. Gordon, P. Miller, 281-289. Chicago, IL: University of Chicago Press.
- Chan, J. 2008. The New Lateral Surveillance and a Culture of Suspicion, In: "Surveillance and Governance: Crime Control and Beyond", *Sociology of Crime, Law and Deviance*, Vol. 10, ed. M. Defflem, 223-239. Bingley, UK: Emerald.
- Cumhuriyet. 2017. Sosyal Medyaya Büyük Operasyon. 14 January. http://www.cumhuriyet.com.tr/haber/siyaset/660327/Sosyal_medyaya_buyuk_operasyon_17_bin_kisi_hakkinda_fezle_ke_hazirlandi_45_bin_kullanici_araniyor.html [Accessed February 18, 2017].
- Ericson, R.V., and K.D. Haggerty. 1997. *Policing the Risk Society*. Oxford: Oxford University Press.
- European Commission for Democracy through Law (Venice Commission), Council of Europe. 2016. *Turkey: Emergency Decree Laws*. [http://www.venice.coe.int/webforms/documents/?pdf=CDL-REF\(2016\)061-e](http://www.venice.coe.int/webforms/documents/?pdf=CDL-REF(2016)061-e) [Accessed March 10, 2017].
- Finkel, A. 2015. *Captured News Media: The Case of Turkey*. CIMA Center for International Media Assistance. <http://www.cima.ned.org/wp-content/uploads/2015/10/CIMA-Captured-News-Media-The-Case-of-Turkey.pdf> [Accessed June 14 2017].
- Freedom House. 2016. *Freedom on the Net 2016: Turkey*. <https://freedomhouse.org/sites/default/files/FOTN%202016%20Turkey.pdf> [Accessed March 3, 2017].
- Icisleri Bakanligi. 2016. *Basin Aciklamasi*. 24 December. <https://www.icisleri.gov.tr/basin-aciklamasi24122016> [Accessed February 20, 2017].
- Kurban, D., and C. Sozeri. 2012. *Caught in the Wheels of Power: The Political, Legal and Economic Constraints on Independent Media and Freedom of the Press in Turkey*. Istanbul, Turkey: TESEV Publications.
- Larsen, M., and J. Piché. 2009. Public Vigilance Campaigns and Participatory Surveillance after 11 September 2001. In: *Surveillance. Power, Problems, and Politics*, eds S. Hier, and J. Greenberg, 187-202. Vancouver, BC: UBC Press.
- Lyon, D. 2001. *Surveillance Society: Monitoring Everyday Life*. Buckingham, UK: Open University Press.
- Lyon, D. 2007. *Surveillance Studies: An Overview*. Malden, MA: Polity Press.

⁸ See Ericson and Haggerty's (1997) argument about the implications of surveillance on institutional parameters of acceptable behavior.

- Marquis-Boire, M., Marczak, B., Guarnieri, C., Scott-Railton, J. 2013. *For Their Eyes Only: The Commercialization of Digital Spying*. Citizen Lab <https://citizenlab.org/2015/10/mapping-finfishers-continuing-proliferation/> [Accessed February 20, 2017].
- Ohm, B. 2015. Organizing Popular Discourse with and against the Media: Notes on the Making of Narendra Modi and Recep Tayyip Erdoğan as Leaders-without-Alternative. *Television & New Media* 16 (4): 370-377.
- Ozeke, H.B. 2014. Turkey: Effects of the New National Intelligence Organization (MIT) Law on Privacy. *Mondaq*, 21 July. <http://www.mondaq.com/turkey/x/328912/Data+Protection+Privacy/Effects+Of+The+New+National+Intelligence+Organization+Mit+Law+On+Privacy> [Accessed February 20, 2017].
- PEN International. 2015. *Surveillance Secrecy and Self-Censorship: New Digital Freedom Challenges in Turkey*. <http://www.pen-international.org/newsitems/turkey-new-report-highlights-declining-space-for-freedom-of-expression-in-the-digital-sphere/> [Accessed March 3, 2017].
- Privacy International. 2014. *The Right to Privacy in Turkey*. <https://www.privacyinternational.org/node/379> [Accessed February 20, 2017].
- Reeves, J. 2012. If You See Something, Say Something: Lateral Surveillance and the Uses of Responsibility. *Surveillance & Society* 10 (3/4): 235-243 [Accessed: March 10, 2017].
- Saka, E. 2014. The AK Party's Social Media Strategy: Controlling the Uncontrollable. *Turkish Review* 4 (4): 418-423 [Accessed: February 18, 2017].
- Saka, E. 2016. Siyasi Trollük Ornegi Olarak Aktroller. *Biririm* (322): 17-21 [Accessed: February 18, 2017].
- Simsek, B., and F. Zengin. 2016. Sanal Teroristlere Sucustu. *Sabah*, 13 December. <http://www.sabah.com.tr/gundem/2016/12/13/sanal-teroristlere-sucustu> [Accessed: March 3, 2017].
- Sozeri, E.K. 2016. Turkey Uses Emergency Decree to Shut Down Internet in 11 Kurdish Cities to Prevent Protests. *The Daily Dot*, 27 October. <http://www.dailydot.com/layer8/turkey-cuts-kurdistan-internet/> [Accessed: March 10, 2017].
- Tasdan, C. 2016. Provokatif Sosyal Medya Hesaplarina Karsi Ihbar Uyarisi. *Anadolu Ajansi*, 18 July. <http://aa.com.tr/tr/15-temmuz-darbe-girisimi/provokatif-sosyal-medya-hesaplarina-karsi-ihbar-uyarisi/610539> [Accessed: March 3, 2017].
- Telli Aydemir, A. 2016. State of Emergency Worsens Digital Crackdown in Turkey. *EDRi European Digital Rights*, 16 November. <https://edri.org/state-of-emergency-worsens-digital-crackdown-in-turkey/> [Accessed March 3, 2017].
- Yeni Safak, 2016. Sosyal Medyada Terore Destek Verenler Nasil Ihbar Edilir? 23 December. <http://www.yenisafak.com/teknoloji/sosyal-medyada-terore-destek-verenler-nasil-ihbar-edilir-2585434> [Accessed: March 10, 2017].
- Yesil, B. 2016. *Media in New Turkey: The Origins of an Authoritarian Neoliberal State*. Urbana-Champaign, IL: University of Illinois Press.
- Yesil, B., E.K. Sozeri, and E. Khazraee. 2017. *Turkey's Internet Policy After the Coup Attempt: The Emergence of a Distributed Network of Online Suppression and Surveillance*. Internet Policy Observatory, University of Pennsylvania. http://globalnetpolicy.org/wp-content/uploads/2017/02/Turkey1_v6-1.pdf [Accessed: February 20, 2017].
- Zeldin, W. 2015. *Turkey: Recent Developments in National and Public Security Law*. The Law Library of Congress, Global Legal Research Center. <https://www.loc.gov/law/help/national-security-law/turkey-recent-developments-2015.pdf> [Accessed: March 10, 2017].