11

Technology, Surveillance, and the Rule of Law in the Digital Age

Dr. Vikasdeep Singh Kohli
Associate Professor
School of Law, Niilm University, Kaithal, Haryana
Vikasdeepsinghkohli@gmail.com

Abstract

Technology changes and disrupts; it enables innovations that spy and collect data, but provides an illusion of security against abuse. The advent of transformative technologies within the surveillance apparatus has prompted questions about adherence to the rule of law, which still leaves room for abuse in democratic societies founded on legality. The state, which has the responsibility of protecting liberty, can turn into a threat to the very liberties it is sworn to secure, by design or circumstance. There have been debates in the contemporary world about the legality, legitimacy, and necessity of data-gathering operations, based on well-established principles grounded in national constitutions and international human rights instruments. It needs a conceptual framework that explores applicable principles and applies them to modern surveillance to evaluate existing regime configurations and possible design alternatives without compromising the rule of law. Technology, Surveillance, and the Rule of Law: Emerging Challenges in the Digital Age fits into this larger project by discussing the systemic regulation of information flows and situating the debate on national-level regimes within a broader national and transnational governance debate. The work explored the topics of technology, surveillance, and the rule of law because they were chosen for their topicality and the presence of an emerging-to-establishment phase. Protection and privacy were omitted since they already receive a broad coverage in available literature (Michael Froomkin, 2000).

Keywords: *Technology and surveillance; rule of law; data governance; privacy and constitutionality; proportionality and safeguards; artificial intelligence and legal regulation.*

1. Introduction

Although digital communication channels are everywhere, the practice of surveillance remains opaque, among individuals and institutions alike. The harm to privacy is not the most severe: a

failed surveillance operation can have a corrosive effect; a stigmatised profile without any legitimate cause may hinder social, economic, and health prospects (Tréguer, 2019). Not only commitments but also legal regimes are required. The surveillance programs should adhere to the statute, not just the form but the spirit; therefore, they should follow the Rule-of-Law principles of legality, availability, transparency, access, and the independent adjudication of conflicts (María García Sanz, 2014). Would you accept surveillance without sufficient regulation of street cameras, drones, or other surveillance technologies? Would that ruin your profile? They require active review, scrutiny, and redress systems to authenticate the validity of reports or profiling in accordance with documented decisions. Surveillance is conducted in shadowy areas, and at times, even when accreditation is provided, it lacks transparency. The best option is to have an accurate, low-risk social profile.

2. Theoretical framework: technology, surveillance and rule of law.

The transformation of predominantly analogue societies into what is currently referred to as the data society often raises concerns about the definition of such a critical term as "society" and the modern reorganisation of pre-existing institutions, organisations, and networks. Technology has become a key element in shaping modern society (Tréguer, 2019). The future of surveillance research is also oriented toward an improved understanding of the relationship between technology and modern society. Using equations, surveillance theories have advanced a typology of forms of surveillance to clarify the conceptual element. Simple surveillance equations are introduced, along with advanced refinements. The famous noisy channel model (Barn and Barn, 2018) reflects the spirit of modern, peripheral cross-society communication. In contrast, modern-day surveillance equations articulate measurements in a less or more comprehensive field. The last surveillance equation opens new opportunities for studying surveillance in the context of multimodal technological objects, caught between entrenched theoretical anchoring and a more general technology-focused approach. Modern society is data- or digital-driven, and whether one prefers the modern categorisation of big data or the Internet of Things, the truth is the same. A data society of this sort may engage multiple stakeholders in dialogues across various sectors of society about data governance, stewardship, management, or control. The act of surveillance, as a process that accompanies the large-scale production of data, is the particular modernity one is experiencing. In this way, it appears to evoke a variety of cultural frames, with data remaining undefined and

surveillance existing concurrently in society, the data society, and data spaces. The investigation of modern-day information monitoring in the economy offers a broader social and situational context.

3. Comparative legislative surveillance regimes.

Surveillance of people can now be ubiquitous, both in public and in private, thanks to technology. The spread of recording devices, biometric recognition technologies, and tracking systems is among the new forms of surveillance enabled by these technologies. The scientific process of gathering, analysing, and sharing information regarding people, groups, nations, or social phenomena is known as surveillance (Tréguer, 2019). The information can include physical characteristics, places, transactions, behaviours, and personal profiles, and is used for monitoring, behaviour modification, security, control, regulation, estimation, assessment, and prediction. The information, on the other hand, is a set of elements that make sense. Surveillance is inherently a matter of knowledge and information, and the study of surveillance is of societal interest because it involves issues of power, control, emancipation, and justice. Current surveillance technologies are increasingly affecting all levels: personal, group, city, national, global, and planetary.

Surveillance of the populace is meant to serve the supposed common good. The government is interested in predicting unwanted occurrences or in fighting back to cause damage to citizens and property. These technologies make people more civil and encourage coexistence; however, they promote degeneration and unchecked surveillance. Mobile devices that use biometrics enable the remote collection of people's private data.

Governments defend the intrusion by claiming that it is done to protect their citizens. Governments limit legal and regulatory frameworks, monopolise the lack of trained personnel and technology, and rely on trusted vendors. Public information, which is easy to reveal and access, is long-term, and private information, which is difficult to access, is temporary.

An overview of the six most populous countries in the world, i.e., China, India, the United States, Indonesia, Pakistan, and Brazil, examines how increasingly interconnected surveillance technologies are being integrated into present-day public services.

4. Protection of constitutionality and privacy.

The accessibility and publicity of personal information have become more possible and widespread through technological solutions: drones, GPS trackers, facial recognition and social

media, which question the old privacy protective doctrine of reasonable expectation (R. Reidenberg, 2014). Such developments challenge the notion that the Constitution grants broad privacy safeguards in the common sphere. Furthermore, the right to the population's privacy is increasingly considered an indispensable condition for the possibility of a fair and orderly rule and enforcement of law and order. The Fourth Amendment protects against unreasonable searches and seizures, while the First Amendment protects rights endangered by government surveillance and data collection.

The boundaries of privacy reflect the growing influence of access and transparency, which have increased substantially over the past several years. It is common practice for people to submit personal data to private enterprises and services, which then spread it and make it publicly available to third parties through social media visibility, retweeting, and applications that gather, accumulate, analyse, and/or distribute it. These constitutive failures have endured amid rising access to information for people and radical changes in existing perceptions, anticipations, and understandings of privacy among the masses.

5. Proportionality, necessity, and safeguards in surveillance

Proportionality and necessity are major principles in government surveillance interference. The proportionality test, which is applied to restrictions of fundamental rights, presents any surveillance action as a three-step test: (i) suitability - the measure under consideration should be able to fulfill the intended purpose; (ii) necessity - the measure under consideration should be minimal among the measures that can serve the same purpose; and (iii) proportionality in its strict sense - the severity of the interference should be balanced with the significance of the pursued purpose (Macnish, 2014). Even a regime that imposes no substantive restrictions on the ends that law enforcement and intelligence agencies might pursue is itself a source of grave rule-of-law concerns. Along with filtering supervision schemes, the public interest may also be represented through a multi-tier scheme, which implies various types of? public interest, including high (life, health), and low (social).

Others procedural controls assume a more prominent role in the structures of accountability other than notification (María García Sanz, 2014) requirements of external authorization, greater ex-post transparency, ex-post monitoring/audit of operations, ex-post evaluation of relevance and data retention, training on how information may be used in a legally permissible way, and proper controls in

case of cross-border/request systems. The appropriateness of these safeguards in practically limiting the acquisition of surveillance, maintaining upstream legitimacy, and preventing upstream overreach is determined by their extent, complementarity, practical implementation, and the overall structure of checks and balances.

6. Control, responsibility and judicial control.

The problem of surveillance and its regulation is twofold in law and politics. Different jurisdictions react in varying ways to surveillance that poses threats to human rights in general and to privacy in particular. An example of such systems is the systems of Brazil and Canada, as they, on the one hand, were made up of statutes, but, on the other hand, the relevant law was perceived as that one which was created, not only initially but also according to the new generations of case law on surveillance (Tréguer, 2019). Accordingly, the courts play a critical yet dependent role that has not yet been fully served by other, more supranational or legislative channels, given the variety of legal systems and operational realities. However, Brazil should also be considered, since, despite certain constitutional standards, the courts have ruled that the right to privacy has a horizontal effect that further limits surveillance in situations where the target is a private actor (Slobogin & Brayne, 2022).

Various jurisdictions have varying ways of controlling surveillance. The rule of law is one of the issues that political actors in newly minted democracies strive to enhance. They make rulings, enact laws, and establish governance systems specifically aimed at reducing the excesses left by previous dictatorial systems. These attempts address the need for political legitimacy, albeit through a well-known form of repression; the goal is not to address the problems of overreach that arise when a broader set of exigencies is considered.

Attempts to address the demographic transition are discouraged by more porous governance systems. The political actors see the continuous externalisation of the state as very beneficial. The extended range of changes being made there is felt well into anticipatory systems throughout the Americas. The twenty-first century began with promises in this direction, in different sectors - constitution-making, electoral reforms, disclosure policies, and regime transitions. However, regimes that could read between the lines of the changing situation could perceive that change was on the verge of occurring; they tried to contain these openings rather than expand them.

7. New technology and legal aspects.

New technologies raise legal issues in the areas of supply chain regulation, risk assessment, and enforcement. Artificial Intelligence (AI) is a central part of supply chains and controls numerous processes at the basic level, also providing intriguing prospects for material and energy replacement. Nevertheless, the legal frameworks governing autonomous AI systems and algorithmically generated products are not yet established, making it difficult to define liability. Even though consumers want increased control, basic rights in AI systems, including Automated Decision-Making (ADM) and Human Intervention (HI), are not formally safeguarded in most cases (Zheng, 2016).

Speaking of the European Privacy Regulation (ePR) and the General Data Protection Regulation (GDPR), biometric technologies play an essential role in identity verification and fraud prevention. The mass implementation of biometric sensors led to a broad-based debate on the regulation, legitimacy and lawfulness (Michael Froomkin, 2000). As they are naturally perimeter-like features, the biometric technical infrastructures form the basis of a sub-category of surveillance. Mobile device and wearable geolocation service imprints affect regulation, particularly in conjunction with cloud computing. Software distribution or Technical Aspects of Interoperability (TAI) Programming interfaces (APIs) that are essential to interoperability catalyse the cross-domain portability of personal data and complementary sharing of usage behaviours and characteristics.

8. Interoperability, data governance and cross-border effects.

Governance of data involves evaluating the design and operation of data-logical systems (Tréguer, 2019). Operable definitions of data governance revolve around three dimensions: protection, fairness, and appropriateness (Hou, 2021). Protection includes information privacy and security. Fairness addresses biases in algorithms and models that make the generation and collection of certain data dangerous. Appropriateness refers to the commercial feasibility and acceptability of data collection. Well-controlled models explain the norms applicable to the particular regime of data processing (e.g., massive collection, information-gathering models, inference). Intermediary forms can be applicable when the models and applications of the data flow across administrative boundaries. Governance architecture explains the institutional domains in which public action occurs, both horizontally and vertically. The law of data governance deals with cyber-surveillance and censitary models. The development of new regulations (e.g., the EU GDPR) points to trends connecting mass databases to the whirls of the

Internet of Things (IoT). The laws already include cross-border transmission, specifying the extent to which transboundary data flows should be filtered, processed, or received. According to such rules, deductive models of transmission, retention, etc. could be selected. Models with identifiers, aggregations and pseudonyms with 12b9f659-5daf-4259-9296-8edff074e3e7 that have superfluous recycling are also suitable for transboundary transmission. Automation of spelling and proofreading, aligned with linguistic data governance, reflects the emerging need to protect linguistic sovereignty, expand transborder pathways, and strengthen infrastructural and cloud-based interactions.

9. Remedies and enforcement, and access to justice.

The implementation is one of the main aspects of governance, including in the digital world. The effectiveness of laws is not based solely on what is in statutes, but also on their implementation. Where legislation is unenforceable, it can become emblematic or unattainable: technical norms, for example, can be specified without the ability to check compliance (Tréguer, 2019). Enforcement is too frequently neglected in technological governance, and much of the focus in that area is usually on the normative strategies of legal definition and regulation. That being said, the following section will evaluate the efficacy of surveillance laws: the institutional, instrumental, and practical arrangements implemented under specific conditions to facilitate adherence to the legal arrangements outlined above and to ensure access to redress in the event of an infraction.

The first stage of departure is associated with the nature of the enforcement mechanisms implemented, which may range from private quantum restrictions and administrative inspections to criminal prosecutions. Although the focus is on disciplinary enforcement systems, there is also attention to the registration, reception, and processing of complaints about illegal surveillance. The second question is the analysis of civil, administrative, and criminal redress avenues available to affected individuals, organisations, or communities. All of them are examined, and the area of the scope of analysis, as well as the type of remedies on offer in various jurisdictions, is of primary concern. The degree to which recourse is administratively easy or not, and financially available or not, is investigated, per route. In addition, in non-legal options such as ethics boards, the ability to provide solutions comparable to the harm inflicted or the threat posed is considered (Calo, 2015).

10. Proportionality, surveillance capitalism and democracy.

Surveillance capitalism is a combination of the economic rationale of the attention economy and an insatiable technological imperative that puts proprietary computation above the value of computational resources. This involves selling all of online and, even more so, offline life by capitalising on the behavioural surplus that arises when users freely share data. The data gathered are no longer subject to rigorous minimisation, as the value of behavioural data cannot be known in advance. Rather, surveillance practices are pervasive and multi-dimensional. Power and accountability will be even more detached regarding the collection, retention, and use of data. The actionable data that may be marketed to third parties is rarely found in clean datasets; instead, it often arises from aggregated traces of interactions among people and groups within complex socio-technical systems. Data that governs the visible data amalgamation by other socio-technical systems, including social media, transport, and search engine systems. Information systems that arrange, organise, localise, synthesise and propagate data assert control over whole populations. The algorithms they implement determine how users perceive their surroundings, navigate, and transform them. However, the invisibility of the datasets themselves limits the ability of data subjects and third parties to question or make sense of the data that is about them. The data one gathers about oneself is subjected to generational cycles of aggregation and transformation, usually in ways that occur below the user's level of consciousness. A lack of clear communication regarding what is being gathered leaves room for mischief, fraud, and misdirection (Tréguer, 2019).

11. Case studies: how it is governed in various jurisdictions.

The above analysis has suggested various approaches to the regulation of surveillance adopted by jurisdictions, showing a high degree of divergence in statutory provisions, control institutions, and judicial interpretation across the European Union and the Council of Europe. In this part, a set of comparative case studies of national and regional systems with striking differences in surveillance governance has been provided, highlighting responses characterised by different levels of innovation, judicial activism, and long-term implementation gaps. Although the cases are chosen not for their representational importance but mainly for their illustrative value, they highlight a wide variety of regulatory possibilities. These cases can provide clues to the efficacy, fragility, and social acceptability of governance remedies that can build regimes of surveillance that are legally responsible, democratically legitimised, and socially advantageous.

The cases under consideration are the legislative reaction taken in Brazil and in the Indian country in the aftermath of the exposure of the mass surveillance after the revelation of the Edward Snowden scandals, and the high-profile rulings that the Court of Justice of the European Union made regarding the lawfulness of the Safe Harbour and Privacy Shield models, which regulated the data flows across the Atlantic. More emphasis is placed on the contrasting outcomes of parallel projects implemented in France and Belgium to amend the legal framework governing the geolocation of mobile phones during the COVID-19 pandemic. It is the variety of these initiatives surveyed that not only sheds light on the ongoing development of governance in relation to surveillance following such landmark events but also clarifies the determinants in the design and implementation of rule-of-law-congruent, technology-based solutions to the urgent and timely problems of surveillance accountability. (Tréguer, 2019)

12. Policy alternatives to enhance the rule of law in surveillance regimes.

The surveillance policies enable governments to intercept data flows across various modalities. The idea of surveillance as a general concept tends to focus on the significance of judicial checks and balances, which is only one aspect of a more intricate power dynamic. Some regimes conduct significant surveillance without judicial oversight, yet still place their nations at the top of the Rule of Law Index. The world has diverse global approaches, and as such, policy alternatives can be developed to enhance the rule of law in surveillance regimes. At three other levels of governance (practice, procedure and principle), specific or targeted policies are suggested. These proposals are based on studies conducted during and after the negotiations between the European Union and the United States (EU-US) on the Datastreams Bridge and Data Privacy Framework. Although not the first to implement the data protection framework, the EU became an initiator of corresponding measures in many jurisdictions. At the individual negotiation stage before the public comment period, policy debates centred on representative issues, indicating the need for appropriate governance frameworks to manage any form of surveillance in other jurisdictions. The EU, therefore, collaborated with other partner countries to avoid dangerous detours whilst enhancing the rule of law in surveillance regimes.

13. Conclusion

Monitoring has emerged as a very popular form of governance in the digital age, attracting the interest of scholars, policymakers, and even civil society. The challenge of unprecedented surveillance

requires urgent academic responses that can frame the problem and inform institutional decisions. The report's retroactive conclusions offer such a framing and investigate how digital surveillance came to be and how it is likely to affect the rule of law in a fast-changing technological environment. Instead of citing digital surveillance, the title of this research mentions technology, which also indicates another problem that should be considered and that is bound to influence further research. The societies are entering a post-digital condition due to the development of artificial intelligence (AI), biometrics, distributed ledger technology (DLT), blockchain, the Internet of Things (IoT) and the metaverse, and other techno-legal innovations that provide societies with radical legal uncertainties, increased rule-of-law risks, and new forms of power and inequality (Tréguer, 2019).

References:

1. Froomkin, A. M. (2000). The death of privacy? *Stanford Law Review, 52*(5), 1461–1543.
2. Tréguer, F. (2019). Seeing like Big Tech: Security assemblages, technology, and the future of state bureaucracy. In D. Bigo, E. Isin, & E. Ruppert (Eds.), *Data politics: Worlds, subjects, rights* (pp. 131–147). Routledge.
3. García Sanz, R. M. (2014). Rethinking privacy to define surveillance. *Revista Internacional de Sociología, 72*(2), 303–324.
4. Barn, B., & Barn, R. (2018). Towards a unified conceptual model for surveillance theories. *Surveillance & Society, 16*(1), 20–39.
5. Reidenberg, J. R. (2014). Privacy in public. *University of Miami Law Review, 69*(4), 101–146.
6. Macnish, K. (2014). Just surveillance? Towards a normative theory of surveillance. *Surveillance & Society, 12*(1), 142–153.
7. Slobogin, C., & Brayne, S. (2022). Surveillance technologies and constitutional law. *Annual Review of Criminology, 5*, 123–141.
8. Zheng, T. (2016). Advanced surveillance technologies: Privacy and evidentiary issues. *International Journal of Law and Information Technology, 24*(3), 226–252.
9. Hou, B. (2021). A novel data governance scheme based on the behavioural economics theory. *Social Science Open Access Repository (SocArXiv)*. https://osf.io/preprints/socarxiv/2b9dc/
10. Calo, R. (2015). Can Americans resist surveillance? *University of Chicago Law Review Dialogue, 82*, 23–34.