DIGITAL AUTHORITARIANISM AND HUMAN RIGHTS: RECONCILING NATIONAL SECURITY AND THE RIGHT TO PRIVACY

Syed Shaharyar Ahmed*

Abstract: Digital technologies are now being used strategically by countries for conducting surveillance, exerting control and repressing people which have given birth to digital authoritarianism. This phenomenon poses severe risks to the international human rights framework, specifically pertaining to the right to privacy as well as the freedom of expression. Governments across the democratic as well as authoritarian systems are rapidly incorporating tools of mass-surveillance, facial recognition mechanisms, data analytics driven by AI, as well as intrusive cyber laws under the guise of national security. This research paper aims to navigate the rift between state security and individual digital rights, such as the right to privacy while assessing how the progressing technologies have removed the barrier between legitimate security interests and systemic violation of human rights. The paper conducts a comparative analysis of legal frameworks across various jurisdictions to determine how digital governance frameworks influence the balance between state independence and human rights. Lastly, the paper suggests a rights-oriented regulatory framework which incorporates accountability, proportionality, as well as privacy-by-design guidelines into the national security system, ensuring that progress in technology is not made at the cost of fundamental rights.

Keywords: Digital Authoritarianism; Digital Surveillance; Mass Surveillance; Human Rights; Digital Rights; Right to Privacy

* Vrije Universiteit Amsterdam, Netherlands.

Table of Contents

Introduction 81

I. Digital Authoritarianism and Human Rights 82

II. Evolution of Digital Surveillance and Security Narratives 84

III. Case Studies: Comparative Perspectives 85

IV. Legal and Ethical Challenges 87

V. Reconciling National Security with Privacy Rights 89

VI. Towards a Normative Framework 91

Conclusion 92

INTRODUCTION

The integration of digital technologies within the sectors of governance, national security as well as law enforcement has occurred at an unprecedented rate in recent years. Although these technologies strive to provide enhanced protection and efficiency, they also pose severe risk of being deployed for discretionary and authoritarian practices. The phrase "digital authoritarianism" refers to this concept as it encompasses the strategic deployment of digital devices by states for conducting mass surveillance, enforcing censorship as well as exerting political control. In contrast to the traditional modes of authoritarianism, wherein reliance is fundamentally placed on hard power and coercion, digital authoritarianism works through a more subtle yet invasive framework which involves manipulation, processing and regulation of information.[1]

The twenty-first century has observed an unprecedented incorporation of digital technologies into the sectors of law enforcement, government as well as national security. Although these technologies strive to provide efficacy, improved security as well as predictive potential, they also carry severe concerns of being deployed for authoritarian use. The term digital authoritarianism refers to this concept. It is basically the strategic deployment of digital technologies by countries for conducting mass surveillance, enforcing censorship, as well as establishing political dominance. In contrast to the traditional modes of authoritarianism, which are mostly dependent on physical dominance, digital authoritarianism works through a more covert yet invasive approach for processing, analyzing and manipulating information. In this regard, the digital landscape has become a platform for not merely national security but also for revamping the power dynamics between the citizens and the state.[2]

The paradigm shift towards digital authoritarianism cannot be separated from the post-9/11 security framework. The terrorist attacks which occurred on 11th of September 2001, led to a seismic shift towards global governance, specifically in the enhancement of national security mechanisms. States across the globe revisited their policies concerning the narrative of counterterrorism, thereby validating extraordinary surveillance mandate under the guise of protecting its citizens. The enactment of USA Patriot Act in the United States, as well as the Investigatory Powers Act in the United Kingdom, and various other counterterrorism legislative frameworks in Europe and Asia demonstrate how national security occupied a key position, even surpassing protection of fundamental freedoms.[3] Surveillance technologies, which were once limited to merely intelligence-based operations, have now been deployed in usual practices and border control, with the validation that digital data collection is required for predicting future attacks. This narrative has validated the breach of right to privacy and other civil protections, which laid the groundwork for digital authoritarianism

---

[1] Tiberiu Dragu & Yonatan Lupu, *Digital Authoritarianism and the Future of Human Rights*, 75 INT'L ORG. 991 (2021).

[2] *Id.*

[3] Orin S. Kerr, *Internet Surveillance Law after the USA Patriot Act: The Big Brother That Isn't* (2002), https://doi.org/10.2139/ssrn.317501.

practices under the guise of national security, even in countries with democratic governments.[4]

The right to privacy has been safeguarded under various international human rights frameworks. For instance, Article 12 of the Universal Declaration of Human Rights (UDHR) provides for protection of individual's liberty, privacy, and family against any unwanted interference. This principle was further reinforced in biding treaties such as under Article 17 of the International Covenant on Civil and Political Rights (ICCPR), which provides protection against unlawful surveillance and mandates the states to safeguard the privacy of individuals from both private and public interference.[5] In the European Legal Framework, the European Convention on Human Rights (ECHR) has provided under Article 8 that the right to privacy and family life needs to be respected and the same has been upheld by the European Court of Human Rights in various landmark judgments. It can be collectively said that these legal frameworks illustrate that privacy is a fundamental right and one of the pillars of a democratic society which ensures freedom, autonomy and dignity.[6]

Despite these safeguards, the emergence of digital technologies has created various gaps between legal frameworks and technological advancements. International human rights law, which was developed decades ago, did not cater to the transformative potential of artificial intelligence, big data analytics or even biometric surveillance. Consequently, while treaties provide for the right to privacy, they lack contextual relevancy while addressing new digital threats like algorithmic profiling, predictive policing as well as automated decision-making.[7] This leads to a severe research gap as to whether legal and policy frameworks reconcile the legitimate national security interests with the need to protect right to privacy and other human rights in a landscape governed by digital technologies? This challenge gets further complicated through the deployment of surveillance technologies by private companies, blurring the distinction between corporate accountability and state responsibility. This research paper will carefully examine how existing legal frameworks regarding human rights can be revisited, reinterpreted or amended so that it could tackle the problems created through digital authoritarianism. Lastly, the research aims to establish that digital advancement does not directly lead towards authoritarianism if adequate legal, ethical, and institutional safeguards are implemented.

I. DIGITAL AUTHORITARIANISM AND HUMAN RIGHTS

Digital authoritarianism has become a global challenge in the digital age, which shows the ways in which governments have deployed digital technologies for exerting influence, suppressing dissent, as well as revamping the relationship between country and its people. There is an interplay of three dominant concepts when studying digital authoritarianism i.e. surveillance authoritarianism, information control and cyber sovereignty. Surveillance authoritarianism refers to conducting pervasive supervision

---

[4] Gabriele Cosentino, *Digital Authoritarianism in the Middle East: Deception, Disinformation and Social Media*, 13 BUSTAN: MIDDLE E. BOOK REV. 190 (2022).
[5] Eliza Watt, *The Right to Privacy and the Future of Mass Surveillance*, 21 INT'L J. HUM. RTS. 773 (2017).
[6] Bart Van Der Sloot, *Decisional Privacy 2.0: The Procedural Requirements Implicit in Article 8 ECHR and Its Potential Impact on Profiling*, 7 INT'L DATA PRIV. L. 190 (2017).
[7] *Id.*

of people and communities through devices such as artificial intelligence-driven facial recognition, data-extracting algorithms as well as biometric identification. These technologies enable states for tracking social trends in real time, which leads to the creation of a "panoptic digital environment". China is the most prominent example of this phenomenon. For instance, through deployment of its advanced networks of surveillance cameras, incorporation of artificial intelligence, and mechanisms like Social Credit Score, the Chinese government has legitimized surveillance is a device for effective governance as well as social engineering.[8]

Information control includes censorship, regulation of online information as well as disinformation practices. It is not just about limiting access towards content but also about revamping the media which is consumed by the citizens. China's "Great Firewall" is an embodiment of this framework. Through scrutinizing foreign websites, limiting access to global sites, and promoting state-sponsored narratives, China has established a self-reliant information ecosystem. Russia has also worked along the same lines which can been seen through the enactment of Sovereign Internet Law of 2019 through which Russia agencies have the mandate to disconnect the Russian part of the internet from the global web, which shows centralized governmental control over digital sharing of information.[9] Lastly, cyber sovereignty is based on the principle that countries should exert complete control over digital activities within their territorial limits, which is similar to the concept of traditional sovereignty. However, the concept is often described as a defensive framework towards foreign interference, while it has been deployed by countries like Iran, Russia and China for validating the restrictive measures for curbing digital freedom. It is interesting to note that digital authoritarianism is not merely confined to authoritarian regimes. Countries with democratic regimes have also started using digital authoritarianism, mostly due to the growing trend of exporting surveillance technologies to these states. For example, Chinese surveillance devices have been used in Latin America as well as Africa, which shows that China has expanded the digital authoritarianism beyond its territorial limits.[10]

The right to privacy along with the freedom of expression are violated when mass surveillance is conducted under digital authoritarianism. Surveillance and censorship collectively violate Article 19 of the ICCPR as well as Article 10 of the ECHR, as both provisions provide freedom for obtaining, receiving as well as sharing information.[11] In this regard, privacy and freedom of expression are mutually relevant and coherent, as people cannot dissent freely without adequate privacy while without freedom of expression, there is no point in having privacy protections. The digital landscape has introduced new technicalities for these rights. For instance, algorithmic profiling as well as predictive analysis violate not only privacy but also the freedom of thought and expression, which potentially halt free speech when individuals are aware that they are under surveillance. In the same manner, mass information collection often

---

[8] Dimitar Lilkov, *Made in China: Tackling Digital Authoritarianism*, 19 EUR. VIEW 110 (2020).

[9] Anna Litvinenko, *Re-Defining Borders Online: Russia's Strategic Narrative on Internet Sovereignty*, 9 MEDIA & COMM. 5 (2021).

[10] Monique Taylor, *China's Digital Authoritarianism* (2022) https://doi.org/10.1007/978-3-031-11252-2.

[11] Amy Shepherd, *Extremism, Free Speech and the Rule of Law: Evaluating the Compliance of Legislation Restricting Extremist Expressions with Article 19 ICCPR*, 33 UTRECHT J. INT'L & EUR. L. 62 (2017).

happens through private companies which provides states with such access, which raises severe concerns regarding human rights and their implementation in the digital ecosystem.[12]

II. EVOLUTION OF DIGITAL SURVEILLANCE AND SECURITY NARRATIVES

The terrorist attacks of September 11, 2001, marked a significant shift towards the evolution of digital surveillance. In the light of these incidents, countries, specifically the United States and the European nations, decided to incorporate sweeping legislative and procedural measures for enhancing national security, mostly at the cost of individual privacy. One of the most fundamental developments was the enactment of the USA Patriot Act in 2001, which largely enhanced the powers of intelligence as well as law enforcement agencies for intercepting communications, obtaining personal records, as well as engaging the bulk surveillance.[13] This legislative framework allowed the National Security Agency (NSA) to implement surveillance mechanisms such as PRISM, which scrutinized email as well as other digital communications of both US residents as well as foreign nationals. Although, labelled as being temporary and extraordinary step, the broad and mostly unchecked authority allowed under these schemes got normalized, which led to the emergency of surveillance exceptionalism.[14]

In Europe, similar trends have been observed, although only through the perspective of data retention and digital surveillance. The European Union Data Retention Directive (2006-2014) allowed telecommunication providers to retain the metadata for specific timeframes for assisting law enforcement agencies. Even though this directive was later scrapped by the European Court of Justice owing to its disproportionate interference with the right to privacy, the directive shows the initial stages of legitimizing mass data collection. Across both regions, the post-9/11 era entrenched the notion that extended surveillance is a justified response towards modern security challenges, therefore, revamping the limitations of state power in the digital landscape.[15]

Although authoritarian regimes have long used surveillance for maintaining social control, democratic states started adopting such procedures which removed the difference between security and authoritarianism. This is often referred to as "creeping authoritarianism". Wherein, apparently temporary security initiatives become part of the permanent institutional protocols. For instance, the expanded police authority, warrantless surveillance as well as algorithmic profiling of people. The normalization of such procedures shows that digital authoritarianism is not limited to autocratic countries but can also manifest in liberal democracies as well under the shadow of

---

[12] Katie Pentney, *The Right of Access to "Reliable" Information Under Article 10 ECHR: From Meagre Beginnings to New Frontiers*, EUR. CONVENTION ON HUM. RTS. L. REV. 1 (2024).
[13] Kerr, *supra* note 3.
[14] Tyler Wall & Torin Monahan, *Surveillance and Violence from Afar: The Politics of Drones and Liminal Security-Scapes*, 15 THEORETICAL CRIMINOLOGY 239 (2011).
[15] Marie-Pierre F. Granger & Kristina Irion, *The Court of Justice and the Data Retention Directive in Digital Rights Ireland: Telling off the EU Legislator and Teaching a Lesson in Privacy and Data Protection*, 39 EUR. L. REV. 834 (2014).

safeguarding citizens against cybercrime or terrorism.[16] Another contextual dimension to this concern is the export of surveillance technologies by western nations to underdeveloped states. Corporations which develop such sophisticated technologies mostly sell these technologies globally including to countries with weak human rights safeguards. For examples, companies in the United States and the European Union, have provided surveillance technologies in Middle Eastern countries for monitoring political activities. The global diffusion of such infrastructure raises severe doubts regarding corporate accountability and the indulgence of democratic regimes in conducting human rights violations.[17]

A new layer to surveillance landscape was added owing to the outbreak of the Covid-19 pandemic, showing how health crisis can enhance the incorporation of digital technologies. Contact tracing applications were deployed across the globe by several states along with digital health passes as well as biometric identification for tracking the infection rate and enforcing quarantines. Although these steps were implemented for ensuring public health and safety, they also led to the creation of certain other problems pertaining to privacy and civil liberties. In contrast to the security measures, pandemic surveillance mostly influenced the entire population, instead of targeting specific group of suspects, which raises doubts regarding the factors or temporality and proportionality. Many contract tracing applications collected in-depth geo-location as well as personal-health information, which was often processed via private platforms in collaboration with governments.[18] In some states, data retention practices lack adequate transparency, with ambiguous collection policies and supervisory frameworks. For instance, reports from various European states mentioned risks pertaining to centralizing sensitive health information without autonomous auditing or judicial scrutiny. The public health ground, though urgent, exposed the ease with which most tools for digital surveillance could be rapidly expanded and normalized, potentially creating standards for conducting future surveillance which might be non-health related. For example, the indefinite retention of metadata as per the post-9/11 mechanisms and the extended data retention during the pandemic highlight the difficult of reversing these measures once they have been legitimized. Furthermore, the reliance towards private companies for obtaining technology further complicates the accountability procedures. Judicial scrutiny and legislative oversight are mostly inadequate where algorithms or corporate platforms are involved, which leads to a governance defect where human rights violations can happen without having access to remedial forums.

III. CASE STUDIES: COMPARATIVE PERSPECTIVES

One of the most advanced and state organized model of digital surveillance is currently being operated by China, where security measures and authoritarian framework converge. Central to this framework is the Social Credit System (SCS), which is a national framework that incorporates fiscal records, online trends as well as interpersonal associations in the form of a unified scoring system. This framework, supported by extended use of facial recognition as well as data integration, awards

---

[16] Marcus Michaelsen, *Far Away, So Close: Transnational Activism, Digital Surveillance and Authoritarian Control in Iran*, 15 SURVEILLANCE & SOC'Y 465 (2017).
[17] *Id*.
[18] Samuel Ribeiro-Navarrete et al., *Towards a New Era of Mass Data Collection: Assessing Pandemic Surveillance Technologies to Preserve User Privacy*, 167 TECHNOLOGICAL FORECASTING & SOC. CHANGE 120681 (2021).

compliance and punishes dissent via limitations on employment, travel as well as access to public spheres. Although the state has framed this system as a device for increasing "trustworthiness" and national security, yet it operates as a mode of systemic repression and behavioral regulation. Its use is more prevalent in the Xinjiang region, where the government has employed mass surveillance tools for controlling the Uyghur people. Technologies include iris scans, DNA sampling, AI-driven predictive policing frameworks as well as facial recognition cameras. China has justified its use under the guise of national security and counter-extremism, through depicting surveillance as a crucial tool for preventing terrorism and social anarchy. However, it has been observed that these initiatives far exceed the principle of proportionality which has been enshrined in the International Human Rights Law.[19]

The European Union has a different framework in which surveillance is incorporated within a robust network of human rights protections, yet rift remains between security measures and privacy safeguards. The incorporation of the General Data Protection Regulation (GDPR) in 2018 has set a global standard in data privacy, establishing guidelines for consent, accountability, as well as data minimization. GDPR aims to provide individuals with digital rights while minimizing the extent of governmental interference with their personal data. Nonetheless, security issues, specifically regarding terrorism, have forced the EU towards extended surveillance frameworks. The revocation of Data Retention Directive by the Court of Justice of the European Union (CJEU) highlighted judicial activism against blanket data retention, however, member states have continued to incorporate legislation which seeks to reincorporate the mass-monitoring framework. Schrems *I (2015)*[20] as well as *Schrems II (2020)*[21] are landmark decisions in this regard through which it was stressed that privacy protections must be ensured during the transatlantic transfer of data. Furthermore, the *Schrems II*, even rendered the EU-US Privacy Shield ineffective owing to concerns regarding the mass-surveillance activities of the United States, elaborating the divergence between American security-focused data retention and European rights-driven frameworks.

The recently enacted Digital Services Act (DSA) as well as the Digital Markets Act (DMA) aim to regulate online content, with a primary focus on transparency, competition as well as accountability. Although not strictly surveillance-oriented laws, they highlight the EU's focus towards improving democratic scrutiny on powerful tech actors which often cooperate with states in activities related to counterterrorism or control of disinformation. Yet, there are some disputes still persistent. It has been observed that counterterrorism directives often push member states to extend their surveillance mechanism in various ways which might be violative of the European Convention on Human Rights (ECHR), specifically the Article 8 (right to private life). The EU framework shows the complications faced by democratic regimes when it comes to balancing security directives with effective human rights safeguards,

---

[19] James Leibold, *Surveillance in China's Xinjiang Region: Ethnic Sorting, Coercion, and Inducement*, 29 J. CONTEMP. CHINA 46 (2019).
[20] Nina Holst-Christensen, *Sag C-498/16 - Maximilian Schrems (1. 2018 Side 52)*, 25 EU-RET & MENNESKERET 52 (2018).
[21] Xavier Tracol, *"Schrems II": The Return of the Privacy Shield*, 39 COMPUTER L. & SECURITY REV. 105484 (2020).

elaborating that even robust legal actions might be forced to compromise privacy when confronted with severe threats.[22]

The surveillance framework of Pakistan as well as the rest of the Global South shows inadequate institutional protections and national security priorities creating opportunities for violations of human rights. Pakistan's security paradigm is heavily dependent on national security legal framework which allows excessive discretionary powers to the intelligence agencies, mostly with minimum judicial oversight. The Prevention of Electronic Crimes Act (PECA) 2016, for example, has enabled the authorities to intercept digital communications under the guise of cybersecurity and counterterrorism. Although it is validated as crucial for combating terrorism and online extremism, PECA has mostly been criticized for its ambiguous provisions, excessive discretionary powers with the potential to be misused against political leaders, journalists or activists. A major shift in Pakistan has occurred after the integration of biometric surveillance system which has been implemented through the National Database and Registration Authority (NADRA). NADRA hosts one of the world's biggest databases for biometric information of citizens, involved in collecting fingerprints, data regarding facial recognition as well as family relationships. Although ostensibly deployed for verification of identity, counterterrorism as well as welfare distribution, the system has created doubts regarding data misuse, insufficient safeguards, and exclusionary measures where members from the marginalized communities are not able to avail such services due to missing biometric information.[23]

In contrast to the EU, Pakistan does not have a comprehensive framework regarding data protection. Draft bills have been circulating ever since 2018, to draft an effective data protection framework, but all of these bills have been criticized for lacking clarity in key rems such as the absence of an independent regulator or providing excessive powers to the government agencies as well as insufficient safeguards against cross-border data transfer. This institutional incompetence has led citizens to be vulnerable against state surveillance, with limited forums for redressal or accountability. Beyond Pakistan, the Global South has shown similar trends, where surveillance technologies are mostly taken from China, Europe or the United States, but used by countries with weaker democratic systems and rule-of-law frameworks. This leads to double vulnerability faced by the masses due to the absence of effective legal protection for human rights and intrusive ability of such imported technologies. The outcome is an increasingly global surveillance divide, where citizens across the Global South are disproportionately vulnerable to uninterrupted surveillance.[24]

IV. LEGAL AND ETHICAL CHALLENGES

The quick development of digital surveillance technologies had led to a lot of ethical and legal concerns, most of which arise from the complication of recalibrating legitimate security risks along with the preservation of human rights. Although governments validate these initiatives under the guise of national security as well as

---

[22] Christoph Busch, *Platform Regulation Beyond DSA and DMA: Which Role for the P2B Regulation?*, 12 J. ANTITRUST ENF'T 201 (2024).

[23] Ihsan Yilmaz and others, *Religious Populism, Cyberspace and Digital Authoritarianism in Asia: India, Indonesia, Malaysia, Pakistan, and Turkey,* (2022) https://doi.org/10.55271/rp0001.

[24] Peter Dauvergne, *Facial Recognition Technology for Policing and Surveillance in the Global South: A Call for Bans*, 43 THIRD WORLD Q. 2325 (2022).

public order, their implementation often strays into the sectors which threaten human dignity, democratic accountability as well as international human rights framework. A prominent legal and ethical dilemma rests in the uncertainty between protection of citizens and monitoring them. Governments mostly utilize surveillance technologies for detecting espionage, terrorism or cybercrime. However, the similar technologies could easily be shifted towards handling political opposition, human rights activists, or even minority segments. For example, under the diverse "anti-extremism" or "anti-terrorism" frameworks, provides that China and Russia have validated mass surveillance campaigns which go beyond valid security concerns, effectively penalizing dissent.[25]

This rift is not confined to authoritarian systems. Even in liberal frameworks, legal instruments often don't possess the adequate precision for prevention of abuse. Uncertain terms like "public order" or "national security" in legislation enables states to unfairly limit rights under the shadow of safeguarding society. From a legal standpoint, this challenges the rules of proportionality and necessity provided in instruments like the International Covenant on Civil and Political Rights (ICCPR). Morally, it causes serious doubts regarding if societies are validating practices which eventually eradicate democratic freedoms.[26]

Another major concern is the extraterritorial nature of surveillance in this digital landscape. The 2013 Snowden revelations exposed the implications of United States along with allied intelligence operations, including the National Security Agency's (NSA) PRISM framework, that collected large cluster of data from users across the globe. Such initiative shows the jurisdictional defects in the domain of international law, where people away from a state's territory are subject to monitoring yet lack locus standi to tackle violations in foreign courts. This leads to a legal vacuum where states have duties under the human rights framework, enforcement is mostly jurisdictional. This outcome is that surveillance mechanisms can target populations from outside jurisdiction with limited scrutiny. European jurisprudence, like the Schrems cases, has attempts to resolve this defect through conditioning information transfers on adequate protections, yet such attempts are mostly limited by region. Extraterritorial surveillance has created a two-tiered system of rights, where citizens have safeguards, while non-citizens are treated as second-class digital subjects, deprived of adequate recourse.[27]

The role of private technology corporation leads to another degree of complexity. Companies such as Meta, Microsoft, Google as well as Amazon usually process, store and collect huge clusters of personal information, making them crucial intermediaries in global governance. Governments mostly rely on these corporation for supplying data or providing access points for mass surveillance. For instance, under the PRISM framework, major United States technology corporations were forced to provide intelligence authorities with access to user data. Apart from compliance with requests from government, corporations themselves actively develop and market surveillance technologies. Companies like the NSO Group, maker of the Pegasus spyware, have allowed authoritarian systems in supervising journalists, opposition

---

[25] Titus Stahl, *Indiscriminate Mass Surveillance and the Public Sphere*, 18 ETHICS & INFO. TECH. 33 (2016).
[26] *Id.*
[27] Marcin Rojszczak, *Extraterritorial Bulk Surveillance After the German BND Act Judgment*, 17 EUR. CONST. L. REV. 53 (2021).

leaders as well as activists.[28] This highlights the profit-based complicity of private actors, in which commercial factors often bypass ethical considerations. Legally, the problem rests in the fragmented regulatory framework while data protection frameworks like the GDPR have imposed obligations, they mostly address consumer privacy instead of the structural strength of Big Tech in allowing digital authoritarianism. Ethically speaking, the reliance on corporate bodies in matters pertaining to fundamental human rights leads to conflicting interests. When surveillance frameworks get privatized, systems for public accountability are weakened, raising doubts regarding fairness, accountability as well as the democratic legitimacy of such systems.[29]

Function creep is the extension of surveillance tools beyond the intended purpose, and it has become another grave concern. Technologies introduced as a response towards legitimate objectives, for instance pandemics or terrorism, are mostly realigned for diverse social or political influence. For instance, contact-tracing applications which were introduced during the phase of COVID-19, were retained or realigned by law enforcement agencies and immigration control. In the same way, national security databases initially intended for tackling counterterrorism might be used for conducting surveillance and monitor political dissents or regulating usual behavior.[30] The same has been observed in the incorporation of China's security devices into the Social Credit System. From a legal perspective, function creep violates the standard of legality, which mandates laws to be precise, reasonably apprehensible, foreseeable as well as evident in their application. When technologies evolve without adequate legal safeguards, citizens are left vulnerable against changing uses which were never democratically allowed. From an ethical standpoint, function creep raises concern regarding the trust in public bodies, the social contract would be devastated if the emergency measures were to achieve permanence as it would lead to skepticism and distrust towards state authority.[31]

V. RECONCILING NATIONAL SECURITY WITH PRIVACY RIGHTS

The problem of striking a balance between individual privacy rights and the national security measures is of the most crucial ethical and legal dilemmas of the digital landscape. Countries have a legitimate objective in protecting citizens against cyber threats, terrorism as well as organized crimes. However, such measures should not violate the fundamental rights provided under the international human rights framework. In order to achieve this harmony, frameworks based on proportionality, scrutiny, technological protections, as well as international collaborate are required. The jurisprudential evolution in the human rights paradigm calls for application of necessity as well as proportionality tests towards surveillance incentives. As per Article 8 of the European Convention on Human Rights (ECHR), the right to privacy can be limited on the grounds of national security, but only if such limitations are "necessary in a democratic state".

---

[28] Gineen K. Abuali, *The Chilling of Religious Liberty in the Age of Digital Surveillance*, 54 SETON HALL L. REV. 533 (2023). <https://doi.org/10.60095/apeg7862>.
[29] *Id.*
[30] Bert-Jaap Koops, *The Concept of Function Creep*, 13 L. INNOVATION & TECH. 29 (2021).
[31] Daithí Mac Síthigh & Mathias Siems, *The Chinese Social Credit System: A Model for Other Countries?*, 82 MOD. L. REV. 1034 (2019).

In the case of *S. and Marper v. United Kingdom (2008)*, the European Court of Human Rights (ECtHR) ruled that retention of DNA samples for an indefinite period, from people not convicted of crimes, violated the vires of Article 8, emphasizing that blanket measures fail the test of proportionality if not done without adequate individualized assessment.[32] Similarly, in the case of *Big Brother Watch v. United Kingdom (2021)*, the Court held that bulk interception frameworks must be coupled with adequate protection mechanisms, such as the inclusion of independent supervision and autonomous authorization for the prevention against being misused. These judgments demonstrate that surveillance incentives need to be modified, target-specific, as well as coupled with robust protections instead of being indiscriminate or excessively diverse.[33]

A second element in reconciling privacy and security rests in the adoption of autonomous oversight and accountability frameworks. Judicial authorization of surveillance measures is a crucial protection against arbitrary encroachment. Furthermore, independent supervisory authorities such as data protection agencies as well as parliamentary intelligence committees are crucial for reviewing state actions. The requirements of transparency would enhance accountability. For instance, annual public reports showcasing the number of surveillance warrants issued enables for effective democratic scrutiny. In the absence of such checks and balances, surveillance risks transforming into a device for exerting political influence rather that ensuring national security.[34]

Other than legal scrutiny, technological incentives can also minimize privacy breaches. For instance, the deployment of Privacy-enhancing technologies (PETs), like differential privacy as well as secured multi-party computation, enables for information to be assessed without exposing the identities of relevant individuals. Encryption is also one of the prominent tools for protecting communications against unwanted interception. Anonymization methods, when properly executed, can also ensure that surveillance mechanisms focus on behavioral patterns instead of identifying individuals. More importantly, incorporating these protections by design, referred to as "privacy by design", allows for protections of human rights, which is a rudimentary principle in deployment of emerging technologies. This approach is in line with the GDPR framework, which ensures data protection through design and by default.[35]

Lastly, to reconcile privacy and national security, there is a dire need for establishing harmonized global standards. Disparities exist in various data protection frameworks which creates confusion, uncertainty, loopholes, thereby allowing states and companies to exploit some jurisdictions. These gaps can be reduced through ensuring international cooperation. The United Nations Human Rights Council (UNHRC) has approved resolutions establishing that the same human rights guaranteed

---

[32] Simon A. Cole, *De-Neutralizing Identification: S. & Marper v. United Kingdom, Biometric Databases, Uniqueness, Privacy and Human Rights*, *in* PALGRAVE MACMILLAN UK EBOOKS (2013), https://doi.org/10.1057/9781137367310_6.

[33] Monika Zalnieriute, *Big Brother Watch and Others v. the United Kingdom*, 116 AM. J. INT'L L. 585 (2022).

[34] Robert G. Patman & Laura Southgate, *National Security and Surveillance: The Public Impact of the GCSB Amendment Bill and the Snowden Revelations in New Zealand*, 31 INTELLIGENCE & NAT'L SECURITY 871 (2015).

[35] Shi-Cho Cha et al., *Privacy Enhancing Technologies in the Internet of Things: Perspectives and Challenges*, 6 IEEE INTERNET OF THINGS J. 2159 (2018).

offline, must also be protected online, thereby urging countries to revisit their surveillance frameworks and ensure compliance with human rights. The Council of Europe has also provided a binding mechanism regarding cross-border data protection in the form of modernized Convention 108+. Similarly, positive benchmarks have been established by the European Union through GDPR and judgments rendered by the Court of Justice, which has revamped the intellectual discourse regarding privacy protections. Without adequate standards, mutual legal assistance and cooperation, there is a severe risk that human rights would be vitiated through divergent privacy frameworks globally.[36]

VI. TOWARDS A NORMATIVE FRAMEWORK

The quick advancement of surveillance technologies as well as their increasing incorporation into the governance frameworks mandates the development of a cohesive normative paradigm which reconciles national security interests with the digital rights safeguards. Existing international frameworks, like the ICCPR as well as the ECHR, allows for foundational guidelines, yet the specific challenges of the digital era such as mass interference, biometric identification, algorithmic profiling as well as cross-border data transfers require a specific approach. For this objective, this research proposes a digital rights-security balance framework, which is targeted around four major pillars of proportionality, temporality, legitimacy and accountability.[37]

For surveillance incentives to be legal, they must be coupled with an accessible and accountable legal framework. Secretive or excessively diverse legislation risks violation both the vires of law and democratic principles. Legitimacy requires law to be clear, foreseeable in its implementation, as well as subject to judicial scrutiny and interpretation. Without this standard, surveillance actions might drift into discretionary misuse or political abuse. Legitimacy ensures that the powers of conducting surveillance are not exercised through emergency or executive measures alone, but rather through a proper channel that is democratic, transparent and which balances national security and rights-oriented protections.[38]

The principle of proportionality restricts the security measures to be within their legitimate limits and do not go beyond what is necessary. Surveillance must be targeted instead of being diversly indiscriminate, limiting the retention as well as collection of user data. Proportionality also mandates that a proper analysis is done regarding the legitimate objective, suitability for achieving it and finding less intrusive methods for obtaining such objective. Incorporating proportionality as a fundamental element in policymaking minimizes the risk of surveillance penetrating the population monitoring under the shadow of national security.[39]

Surveillance regimes need to be subjected to autonomous supervision mechanisms which could monitor compliance, prevent misuse as well as provide remedies for people whose rights have been violated. Accountability can operate on

---

[36] Francesca Bignami & Giorgio Resta, *Human Rights Extraterritoriality: The Right to Privacy and National Security Surveillance* (2018), https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID3043771_code810317.pdf.

[37] *Id.*

[38] Peter Königs, *Government Surveillance, Privacy, and Legitimacy*, 35 PHIL. & TECH. (2022).

[39] *Id.*

various levels such as judicial authorization for intrusive actions, parliamentary supervision of intelligence authorities as well as robust data protection agencies empowered to analyze complaints. Furthermore, remedies should be accessible and efficient, individuals must have the right to seek redressal against unlawful surveillance, both nationally and internationally through platforms like UN Human Rights Committee or ECtHR. Without transparency, even ideally crafted laws could risk getting ignored in practice.[40]

Lastly, surveillance mechanisms should be limited by time and there should be periodic review assessments. Exceptional circumstances often could entail such measures as response to crises like in times of pandemic or terrorism, however this should lead the surveillance actions to gain permanence. Temporality tackles the threat of "function creep" through mandating governments for justifying the renewal of such powers, subjecting them to independent scrutiny and democratic oversight. Furthermore, temporality ensures that technologies introduced for purposes like contract-tracing during COVID-19, do not gain permanence as tools for exerting state control.

CONCLUSION

It can be conclusively said that the emergence of digital authoritarianism depicts one of the defining issues of the 21st century, revamping the canons of governance, personal freedom, and the international human rights framework. As states extend their dependence on surveillance technologies and data-oriented decision-making under the umbrella of national security, the delicate balance among collective security and personal rights faces severe strain. This research has highlighted that although technological innovation offers powerful tools to the sates for addressing concerns such as cybercrime, pandemics as well as terrorism, it also leads to the creation of new risks associated with violation of human rights, repression as well as democratic backsliding. The core issue lies not in if surveillance should be allowed, but in how it could be regulated so that legitimate security interests are addressed without violating the right to privacy and related human rights.

This research has elaborated how various jurisdictions have dealt with this issue. Authoritarian systems, exemplified through China's Social Credit System as well as extended use of biometric monitoring, deploy digital devices for institutionalizing control, often under the shadow of national security. Democratic systems, although formally committed towards granting human rights safeguards, have also drifted towards "creeping authoritarianism" through the extension of surveillance authority, as observed in the post-9/11 ecosystem in the United States and the counterterrorism systems of the European Union. The case of Pakistan as well as other Global South countries highlight the concerns where weak institutional protections and underdeveloped data protection frameworks leave citizens prone to state trespass and foreign surveillance. These comparative perspectives establish that the distinction between authoritarian and democratic digital trends in digital methods has been blurred, highlighting the dire need of legislative and normative reforms.

---

[40] Arnaud Braud et al., *The Road to European Digital Sovereignty with Gaia-X and IDSA*, 35 IEEE NETWORK 4 (2021).

This research has proposed a Digital Rights-Security Balance framework, which is based on the principles of legitimacy, accountability, proportionality as well as temporality. These standards collectively ensure that surveillance mechanisms are legally sound, narrowly crafted, and independently scrutinized, which being subject to review or sunset clauses. More importantly, this framework stresses that privacy protection is equally important as national security, as privacy boosts trust in state authorities, allowing for collaboration and resilience against genuine threats. Furthermore, international collaboration through frameworks such as the GDPR, Council of Europe Conventions, is necessary for preventing excessive surveillance by states.

Lastly, the struggle against digital authoritarianism is also for the protection of democratic norms in the digital landscape. Through incorporating robust protections into the regulatory as well as legal frameworks, societies can tackle the normalization of surveillance exceptionalism while ensuring universal application of human rights. The objective is not just to regulate technology, but rather to make sure that technological strength serves humanity instead of subjugating it. In achieving such objective, the international community needs to carve a path where security and human rights are not seen as competing interests, but as mutually reinforcing canons of a fair and democratic digital landscape.

(Student Editor for this Article: Ersai Fan)