ESTABLISHING A HARMONIOUS BALANCE BETWEEN HUMAN RIGHTS LAW AND DIGITAL MASS SURVEILLANCE*

İnsan Hakları Hukuku ile Dijital Kitlesel Gözetim Arasında Uyumlu Bir Denge Kurmak

Melih Uğraş EROL**

L&JR
Year: 17, Issue: 31
January 2026
pp.1-26

Article Information

Submitted : 3.4.2025
Revision Requested : 22.7.2025
Last Version Received : 23.7.2025
Accepted : 30.10.2025

Article Type

Research Article

Abstract

Global and regional human rights authorities counsel nations to refrain from engaging in arbitrary, discriminate, and unlawful digital mass (bulk) surveillance. However, the interaction of digital mass surveillance with preventing crime, thwarting human exploitation, and safeguarding human rights creates a complex and dual-edged relationship. The collaboration between governments and private enterprises in the realm of monitoring individuals elevates the discourse surrounding digital mass surveillance beyond the confines of conventional governance and political frameworks. In order to acknowledge the relationship between human rights and digital mass surveillance, it is crucial to recognise their differences. It is crucial to establish a multi-stakeholder governance framework that effectively protects human rights and fosters accountability. Consequently, a harmonious balance strategy can be constructed to reconcile digital mass surveillance with the preservation of human rights and freedoms, ensuring that neither is unduly compromised.

Keywords: Digital mass surveillance, human rights, human exploitation, crime

Özet

Küresel ve bölgesel insan hakları otoriteleri devletlere keyfi, ayrım gözeten ve hukuka aykırı dijital kitlesel gözetlemelerden kaçınmalarını tavsiye etmektedir. Ancak, dijital kitlesel gözetlemenin suçun önlenmesi, insan istismarının engellenmesi ve insan haklarının korunması ile

* There is no requirement of Ethics Committee Approval for this study.

** Dr., Rauf Denktaş University, Faculty of Law, E-Mail: melihugras.erol@rdu.edu.tr, ORCID ID: 0009-0006-9905-8633.

etkileşimi karmaşık ve iki uçlu bir ilişki yaratmaktadır. Bireyleri izleme alanında hükûmetler ve özel teşebbüsler arasındaki iş birliği, dijital kitlesel gözetimi çevreleyen söylemi geleneksel yönetişim ve siyasi çerçevelerin sınırlarının ötesine taşımaktadır. İnsan hakları ve dijital kitlesel gözetim arasındaki ilişkiyi kabul etmek için aralarındaki farkları tanımak çok önemlidir. İnsan haklarını etkin bir şekilde koruyan ve hesap verebilirliği teşvik eden çok paydaşlı bir yönetişim çerçevesi oluşturmak şarttır. Sonuç olarak, dijital kitlesel gözetleme ile insan hak ve özgürlüklerinin korunmasını uzlaştırmak için uyumlu bir denge stratejisi oluşturulabilir ve böylece her ikisinin tehlikeye atılmaması sağlanabilir.

Anahtar Kelimeler: Dijital kitlesel gözetim, insan hakları, insan istismarı, suç

Introduction

The notion of "the right to be let alone"[1] was articulated by Judge Colly in 1888, originally conceived as a safeguard against physical torts. Progressively, the right has developed to include safeguarding of personal privacy and components of a legal structure for confidentiality and privacy.[2] The right to privacy is exceeding mere property considerations and encompassing the broader right to fully experience and enjoy life. The most comprehensive interpretation of the privacy as a human right in the contemporary understanding is the right to remain undisturbed.[3] This comprehension indicates that the privacy as a human right is acknowledged as a civil liberty and the concept has indeed evolved from Colly's perspective. In contrast, the present circumstances are indicative of a perpetual cycle in which the concept of privacy is attempting to establish its position within the digital realm, while dialogues concerning cyber-digital-e-mass surveillance pertaining to this right continue simultaneously.[4]

The interconnectedness of the cyber landscape, technological advancements, and the progression of communication methods with human rights is irrefutable.[5] The discussion regarding mass surveillance and human rights in cyberspace continues to be a provocative topic within the realm of human rights law. Legal developments on this subject are ongoing, and efforts are focused on establishing a universally recognised legal framework.

---

1 Thomas M. Cooley, *A Treatise on the Law of Torts, or the Wrongs Which Arise Independent of Contract* (Callaghan & Co 1888) 29.

2 Irwin R Kramer, 'The Birth of Privacy Law: A Century Since Warren and Brandeis' (1990) 39 Cath U L Rev 703, 703-724.

3 Samuel D Warren and Louis D Brandeis, 'The Right to Privacy' (1890) 4 Harv L Rev 193.

4 Ibid 193.

5 See Dapo Akande and others (eds), *Human Rights and 21st Century Challenges: Poverty, Conflict, and the Environment* (OUP 2020).

There are relevant issues regarding the convergence of digital mass surveillance and human rights. Initially, the function of digital landscapes in the realms of crime prevention, human exploitation prompts an inquiry into the interplay between digital mass surveillance and safeguarding human rights.[6] Considering the various types of information collected through intelligence operations, especially through untargeted digital mass surveillance, it becomes clear that this method of surveillance poses substantial concerns about its effects on people, notably social and religious minorities.[7] Unfortunately, the prevalence of security concerns frequently results in nations sacrificing human rights and individual freedoms in the context of digital mass surveillance.

The implementation of mass surveillance as a means to tackle security issues prompts significant apprehensions regarding the possible exploitation of the gathered data for nefarious ends.[8] Under these conditions, surveillance can stimulate discourse regarding its validity as a means of safeguarding human life and security or as a potential infringement on rights and freedoms, which could result in a constrained application of communication and its technologies.[9] The imperative of this form of surveillance for the preservation of national security continues to be a subject of persistent discourse.

Digital mass surveillance must be comprehended with both benefits and drawbacks.[10] The notion of digital mass surveillance has progressively infiltrated human existence, propelled by the development of technology, which has concurrently merged with societal oversight within the digital domain. The tension between human rights and freedoms, security anxieties and digital mass surveillance constitutes the paramount balance-necessitated discussions in the digital concept.[11]

---

6 See Marcin Rojszczak, *Bulk Surveillance, Democracy and Human Rights Law in Europe: A Comparative Perspective* (Routledge 2025).

7 Ibid 12.

8 Theodore Christakis and Katia Bouslimani, 'National Security, Surveillance, and Human Rights' in Robin Geiß and Nils Melzer (eds), *The Oxford Handbook of the International Law of Global Security* (OUP 2021) 699.

9 Giovanni Ziccardi, *Resistance, Liberation Technology and Human Rights in the Digital Age* (Springer 2013) 202.

10 For the debates on digital mass surveillance see: Jacopo Bellasio and others, 'The Future of Cybercrime in Light of Technology Developments' (RAND 2020); Peter Swire, 'The Second Wave of Global Privacy Protection: Symposium Introduction' (2013) 74 Ohio St LJ 841. David Lyon, *The Electronic Eye: The Rise of Surveillance Societies* (Polity 1994); David Lyon, *Surveillance Society: Monitoring Everyday Life* (Open University 2001).

11 See David Lyon, *Surveillance Studies* (Kalkedon 2013).

1. Human Rights in the Glance of Digital Mass Surveillance

The mechanisms of automatic data processing, thereby instituting a legal concept to protect private data and addressing pertinent issues that are connected in the human rights framework.[12] The implementation of these surveillance techniques and ongoing operations, devoid of sufficient protections for human rights, has elicited significant apprehension.[13] In accordance with human rights states must avoid engaging in mass surveillance activities that are arbitrary or unlawful.[14] Specifically, the practice of untargeted mass surveillance, when assessed alongside the safeguarding of private life and personal data, poses a threat to human rights. To address human rights concerns, there is a clear necessity for governmental mass surveillance activities to be attached in a legal framework and executed in alignment with clear and established laws.[15] It is incumbent upon states to guarantee that any encroachment upon individual privacy, encompassing mass surveillance and the sharing of intelligence, is in accordance with international human rights law.[16]

Over time, the need to better accommodate emerging technologies directed human rights law normative frameworks to develop through highlighting the importance of informational autonomy, reinforcing the rights of data subjects, and underscores the principle of proportionality in the realm of data processing.[17] The intrinsic connection concentrates on the safeguarding of human rights and human dignity, and the fundamental principles governing digital mass surveillance, which include legality, necessity, proportionality, and transparency. These principles ensure the legitimacy of the digital mass surveillance operations, emphasising the importance of informing citizens about the matter and securing access to appropriate legal remedies in instances of unlawful actions.[18] The necessity

---

12 Council of Europe (CoE) 'Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data' <https://rm.coe.int/1680078b37> accessed 2 April 2025.

13 United Nations (UN) 'Report of the General Assembly on the Seventy-Third Session: Right to Privacy, UN Doc A/73/4382' (17 October 2018) 4 <https://documents.un.org/doc/undoc/gen/n18/324/46/pdf/n1832446.pdf> accessed 12 March 2025.

14 United Nations Human Rights Council 'Report of the Human Rights Council on Its Thirty-Ninth Session: The Right to Privacy in the Digital Age UN Doc A/HRC/39/29' (3 August 2018) <https://www.ohchr.org/sites/default/files/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/A_HRC_39_29_EN.pdf> 4 accessed 12 March 2025.

15 Ibid.

16 Ibid.

17 Cecile de Terwangne, 'Council of Europe Convention 108+: A Modernised International Treaty for the Protection of Personal Data' (2021) 40 Computer Law & Security Review 105553 <https://www.sciencedirect.com/science/article/abs/pii/S0267364920301023> accessed 10 March 2025.

18 Council of Europe 'Convention 108+' (2018).

of limited purpose in digital mass surveillance and storage of collected data, the minimisation of collected data volume, and the emphasis on accuracy are significant considerations in the effort to combat cybercrime and protect human rights.[19] Collection and retention of personal data, the interception of content data, the legality of location data collection and retention encompass legitimate aims of digital mass surveillance.[20] These measures improve the investigation and prosecution of cybercrimes while also ensuring that mass surveillance practices conform to the principles such as necessity, proportionality and transparency.

Digital mass surveillance is applicable in strict necessity and states are obliged to rigorously examine such surveillance to ensure the safeguarding right to privacy and the protection of personal data.[21] The requisite elements must be established to satisfy the legal criteria, encompassing the identification of individuals subjected to digital mass surveillance, temporal constraints, and protocols regulating the examination, utilisation, and retention of collected data. From a perspective focused on human rights, it is essential for governments to define explicit regulations regarding authorisation procedures, the judicious implementation of digital mass surveillance, the duration of data retention, and the protocols for sharing data with external entities.[22] The implementation of comprehensive safeguards is essential to avert abuse and misuse of digital mass surveillance opportunities; failing to do so may lead to significant repercussions that contravene human rights law.[23] Given the current legal discussions and the practical difficulties inherent in digital mass surveillance, these practices must adhere to strict and clearly defined guidelines to prevent any infringement on human rights.

The regional and international law texts have pioneered developments in the realm of digital law and in European Union's (EU) legal framework, articulated through the General Data Protection Regulation (GDPR) and the EU Charter of Fundamental Rights, ensures transparency, equity, and the legitimacy of surveillance methods. The confidentiality of communications aligns with international human rights standards and the constitutions of Member States of EU, as explicitly had already articulated in the ePrivacy Directive issued by the European Parliament and Council on July 12, 2002. The directive under consideration advocates for heightened awareness of the issue across the electronic communications sector and exemplifies the collaborative efforts required from various stakeholders.

---

19 Council of Europe 'Convention on Cybercrime' (2001).

20 *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* [2014] ECLI [C], para. 317.

21 *Szabó and Vissy v. Hungary* [2016] ECtHR [GC] 37138/14, para. 71-72.

22 Ibid.

23 *Weber and Saravia v. Germany* [2006] ECtHR [GC] 54934/00, para 95.

Recently, there has been a debate on how to balance the protection of individual rights but also combat crimes and focus on the identification and reporting of child sexual abuse material (CSAM) across online platforms within internet users' private communications in EU.[24] The objective of a proposed regulation by the European Parliament and Council establishes comprehensive guidelines at safeguarding children from sexual abuse in both digital and physical environments, which aligns with the principles articulated in the United Nations(UN) and EU human rights law texts.[25] The essentiality of safeguarding children against abuse, necessitates a series of actions, one of which involves internet providers potentially employing digital mass surveillance as a means to report any instances of abuse. The proposed system has faced scrutiny, despite its declared intention to prioritise the welfare of children and combat crime, particularly concerning potential infringements on human rights, especially privacy. A collective of 379 scientists and researchers hailing from 36 nations has articulated their concerns regarding this measure in an open letter.[26] Their findings clarified the plan's framework, which infringes upon the essential right to privacy and presents a significant potential for indiscriminate and disproportionate digital mass surveillance. Moreover, to enhance the surveillance capabilities of Member States of EU and Europol, has raised concerns regarding the potential erosion of human rights, especially in the context of immigration.[27] Civil society initiatives within the EU are actively involved in the endeavour to constitutionalise mass surveillance for respecting rights of people.[28] Civil society organisations within the EU also argue that the persistent inadequacies of digital mass surveillance in effectively tackling issues warrant the cessation of its expansion.[29] The apprehensions expressed by civil society regarding the

[24] For the debates see European Digital Rights, 'Utopian Dreams, Sobering Reality: The End We Start From In EU's Approach To Technology' (2 April 2025) <https://edri.org/our-work/utopian-dreams-sobering-reality-the-end-we-start-from-in-eus-approach-to-technology/> accessed 2 April 2025.

[25] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council Laying Down Rules to Prevent and Combat Child Sexual Abuse' COM (2022) 209 final <https://eur-lex.europa.eu/resource.html?uri=cellar:13e33abf-d209-11ec-a95f-01aa75ed71a1.0001.02/DOC_1&format=PDF> accessed 14 March 2025.

[26] Open Letter <https://nce.mpi-sp.org/index.php/s/eqjiKaAw9yYQF87> accessed 10 March 2025.

[27] European Digital Rights, 'Why The New Europol Regulation Is A Trojan Horse For Surveillance' (5 March 2025) https://edri.org/our-work/why-the-new-europol-regulation-is-a-trojan-horse-for-surveillance/ accessed 2 April 2025.

[28] Edoardo Celeste and Giulia Formici, 'Constitutionalizing Mass Surveillance in the EU: Civil Society Demands, Judicial Activism, and Legislative Inertia' (2024) 25 German LJ 427.

[29] DiEM25 Communications,'The EU's Orwellian Agenda: Using Child Protection to Justify Mass Surveillance' (08 October 2024) <https://diem25.org/the-eus-orwellian-agenda-using-child-protection-to-justify-mass-surveillance/> accessed 10 February 2025.

digital mass surveillance strategy within the EU highlight the potential for exacerbating discrimination, injustice, and oppression, ultimately functioning as a tool for the misuse of authority. The jurisprudence of the CJEU has served as the principal driver for constitutionalising, as it has judiciously concluded that a blanket ban on mass surveillance is not a practical solution.[30] The legal analyses in EU illustrate a nuanced interaction between the national security and human rights law. The absence of clarity surrounding digital mass surveillance practices in EU, coupled with the potential for these measures to be contradicting human rights, ultimately undermines the balance between digital mass surveillance and fundamental rights. In this framework, to a legitimate digital mass surveillance the principles of data security and digital mass surveillance must adhere to the tenets of legality, necessity, proportionality and transparency within a democratic society.[31] It is imperative that Member States provide adequate and effective safeguards against potential abuses in the event of any infractions. The discourse seems to be continued, even though these efforts have yet to yield a distinctly articulated resolution within the EU.

2. Human Rights Law Landmark Cases from Two Continents

Two significant cases from different continents have contributed to the debate regarding the balance between the politics of digital mass surveillance and personal rights, particularly as a part of the ongoing discussion surrounding the essential legal praxis on this issue. The North American case *Carpenter v. United States* and the decision given by the European Court of Human Rights (ECtHR) in *Big Brother Watch and Others v. The United Kingdom* and *Centrum För Rättvisa v Sweden* cases exemplify how digitisation poses new challenges to established concepts of human rights, highlighting the tension between fundamental liberties and state-sanctioned mass surveillance.

The United States Supreme Court's ruling in *Carpenter v. United States* meticulously scrutinised the ramifications of privacy rights in the digital era. The case meticulously scrutinises the data gathered from cellular phone locations. The authorities acquired the location data of the defendants' cell phones spanning several months during a criminal investigation carried out in Detroit in 2011. This incident occurred without an antecedent inquiry into probable cause. The information regarding an individual identified as Timothy Carpenter consists of 12,898 distinct location data points. This statistic indicates an average of 101 location data points discerned each day throughout a duration of four months. The matter was brought before the Supreme Court on November 29, 2017, for consideration. Carpenter challenged his conviction, which was partially based on the location data obtained from his mobile phone. The government employed

30 *Ireland v. European Parliament and Council* [2009] ECR I-00593.

31 For the details see: *Centrum För Rättvisa v Sweden* [2016] ECtHR [GC] 35252/08.

legislation that requires a court order grounded in "reasonable grounds" rather than probable cause, thereby enabling the acquisition of this information without the necessity of a search warrant. The authorities used the digital data at their disposal to meticulously analyse the past and conduct thorough digital surveillance concerning the matter previously addressed. The authorities carried out this action without obtaining a court order on valid grounds, which led the court to determine its illegality. A crucial element of the decision that could set a precedent is the absence of consideration for the third-party doctrine in the decision-making process. This notion carries considerable weight for the advancement of digital technology and safeguarding human rights, despite its application by courts in the United States. Those who opt to disclose information to external entities cannot justifiably anticipate privacy concerning that information, as delineated by the pertinent legal doctrines. The failure to effectively identify and monitor these signals resulted in the determination that the execution of this method was flawed. This decision is pivotal in assessing the enhancement of digital monitoring and safeguarding human rights in the contemporary digital landscape, as well as in implementing measures to safeguard personal information. The court case at hand exemplifies the need to assess the legal standards governing data and surveillance obtained through digital means, considering the protection of personal information alongside the requirement for compelling and justifiable reasons. The prior reference to the judicial decision substantiates this claim.[32]

On the European continent, the decision rendered by the ECtHR in *Big Brother Watch and Others v. The United Kingdom* is deeply intertwined with the implications of the Snowden affair. This case is significant due to the widely reported revelation of NSA documents to the media by Edward Snowden, a former employee of both the Central Intelligence Agency (CIA) and the National Security Agency (NSA). The disclosures illuminated the extensive scope of international surveillance initiatives conducted by the NSA. The operation of the TEMPORA program by the Government Communications Headquarters (GCHQ) holds particular importance for the United Kingdom, as it involves mass interception in collaboration with U.S. intelligence, thereby enabling the gathering data of communications from service providers.[33] Consequently, the civil society organisation Big Brothers et al. submitted an application to

[32] For the case see: *Carpenter v. United States* [2017] Supreme Court of United States No. 16–402 <https://cdn.cnn.com/cnn/2018/images/06/22/16-402_h315.pdf> accessed 2 April 2025.

[33] *Big Brothers and others v. United Kingdom* [2021] ECtHR [GC] 58170/13, 62322/14 and 24960/15 para 2: "The Edward Snowden revelations made in 2013 indicated that Government Communications Headquarters ("GCHQ", being one of the United Kingdom intelligence services) was running an operation, codenamed "TEMPORA", which allowed it to tap into and store huge volumes of data drawn from bearers. The United Kingdom authorities neither confirmed nor denied the existence of an operation codenamed TEMPORA."

the ECtHR following the Snowden revelations, asserting that the surveillance infringed upon the rights to privacy and freedom of expression. The ECtHR ultimately determined that there had been a violation of Article 8, respect for private life, and Article 10, freedom of expression, in the practices of the UK.

The case of *Centrum För Rättvisa v Sweden* centres on the claim that Sweden's legislation allowing the Swedish National Defence Radio Establishment (FRA) to perform mass surveillance of electronic communications and engage in signal intelligence practices infringes upon Article 8 of the ECHR. The ECtHR, while taking a measured stance on the mass surveillance issue, underscored that the practice in Sweden included adequate and effective guarantees. The court has assessed the judicial pre-authorisation procedure and the independent body's oversight of the surveillance in question in accordance with Article 8. Nonetheless, the court highlighted the necessity for more defined regulations and protocols concerning the storage, destruction, and dissemination of the acquired data, and the importance of enhancing aspects like transparency and accountability has been highlighted. This decision is important since its establishment as a precedent in Europe, allowing states to engage in mass signal intelligence programs while adhering to stringent conditions that safeguard fundamental human rights. According to the decision, a mass surveillance framework may be considered acceptable from a human rights perspective, contingent upon the presence of legal safeguards, independent oversight, and explicit procedural guarantees.[34]

The Court underscored that mass surveillance could be relevant under specific conditions. In the context of the *Weber and Saravia v. Germany* case, which marked a significant aspect in the realm of human rights law. Six requirements established by the Court for lawful mass surveillance: (i) the law must restrict the offences that warrant mass surveillance in order to prevent its unnecessary use; (ii) the target group of the mass surveillance must be limited to prevent indiscriminate surveillance; (iii) the timing of the mass surveillance must be limited in order to prevent endless monitoring of individuals; (iv) procedures for handling the obtained data must be in place to protect procedural guarantees; (v) safeguards must be taken when communicating data with third parties in order to prevent the use of obtained data outside of the law; (vi) essential limits must be adopted for data minimisation and timely erasure in order to mitigate the effects of surveillance. [35] In the case law the Court has also delineated several stipulations referred to as "end-to-end safeguards" to guarantee that extensive surveillance does not once more result in the infringement of human rights. In this context, the states must recognise the presence of an evaluation mechanism at every phase of the process of digital mass surveillance. This assessment

34 *Centrum För Rättvisa v Sweden (n 31).*

35 *Weber and Saravia v. Germany* (n 23) para.96.

framework pertains to the necessity and proportionality of the surveillance being executed, and the probability of individuals experiencing infringements of their rights will be remedied. Furthermore, when delineating the objective and extent of the operation, the requirement for independent authorisation from the outset might mitigate arbitrariness, as the activity ought to be overseen and subjected to an independent, ex post facto evaluation.[36]

The regulations, interpretations, and norms regarding digital mass surveillance in human rights law are very recent. The emergence of the digital era has necessitated an increased emphasis on this topic across all legal systems. The objective is to achieve a balance between individual rights and state programs, as well as social interests and security.

3. The Dichotomy of Digital Mass Surveillance, Human Exploitation and Prevent Crime

9/11 attacks shaped the evolution of global security measures, strategies for crime prevention, and the public's acceptance of mass surveillance initiatives.[37] Since then, security and the attainment of peace are accepted as fundamentally interdependent and states have exercised considerable discretion in relation to digital mass surveillance, especially as state institutions have highlighted the global dangers associated with terrorism and international crime.[38] States have responsibilities under human rights law to ensure that individuals can exist in peace and with dignity while addressing global challenges. In this context, the implementation of digital mass monitoring could potentially curtail personal liberties, all while ostensibly striving to safeguard societal interests and collect data through digital mass surveillance that transcends physical boundaries.[39] This digital mass strategy embodies the conceptual framework of the panopticon, cultivating discipline through an awareness of continuous observation.[40] Individuals perceive themselves as subjects of scrutiny while the observer remains hidden from view.[41] Nevertheless, the understanding of the panopticon framework has evolved into discussions surrounding the post-panopticon paradigm in the digital

---

36 *Big Brothers and others v. United Kingdom* (n 33).

37 Lyon (n 11) 28.

38 Andrian Bogdan, 'The Right to Peace in the Context of Contemporary International Reality' (2013) 40 Revista de Stiinte Politice 46.

39 Maša Galič, Tjerk Timan and Bert-Jaap Koops, 'Surveillance Theory and Its Implications for Law' in Roger Brownsword, Eloise Scotford and Karen Yeung (eds), *Oxford Handbook of the Law and Regulation of Technology* (OUP 2017) 731.

40 Jeremy Bentham, *The Panopticon Writings* (Verso 1995).

41 Donna Susan Mathew, 'Surveillance Society: Panopticon in the Age of Digital Media' *The New Polis* (19 May 2020) <https://thenewpolis.com/2020/05/19/surveillance-society-panopticon-in-the-age-of-digital-media-donna-susan-mathew-part-2/> accessed 10 February 2025.

society.[42] The post-panopticon understanding employs advanced technologies such as closed-circuit television, biometrics, smart devices, blockchain, and social media to facilitate extensive digital mass surveillance.

In practice important questions arise regarding the relationship between digital mass surveillance, the prevention of crime, which is accepted as a legitimate aim of digital mass surveillance, and the safeguarding people's life. A set of current global data indicates that the relationship between the density of cameras in closed-circuit television systems and crime rates is far more complex than previously understood.[43] Evidence indicates that the efficacy of crime prevention cannot be solely attributed to digital mass surveillance. The proliferation of digital mass surveillance cameras does not invariably correlate with a reduction in crime rates, as there exists a minimal relationship between the number of cameras and a decrease in the crime index.[44] However, the foundational tenets of legality, applicability, and data security are essential to achieve a legitimate aim of crime prevention and apply digital mass surveillance. The digital mass surveillance against crimes may intricately link to the fundamental right to life, within the broader context of human security and enjoyment of all human rights. The right to life serves as the foundation for realising all other human rights in the indivisibility and mutual reliance of human rights. It is incumbent upon states to ensure the protection of individuals from threats that may jeopardise their fundamental rights to life.[45] In this context, digital mass surveillance may be construed as a human rights obligation for states when examined comprehensively, and these applications could be regarded as instruments employed by states to safeguard the fundamental right to life in the prevention of life-threatening crimes.[46] While digital mass monitoring initiatives have been implemented to deter crime and capture offenders, these strategies are anticipated to suppress prospective future criminal behaviour.[47] Nevertheless, these applications often involve the categorisation of individuals based on specific socioeconomic conditions or geographic locations, which consequently makes them vulnerable to biases and discriminatory practices.[48]

---

42 William Bogard, 'Simulation and Post-Panopticism' in Kirstie Ball, Kevin Haggerty and David Lyon (eds), *Routledge Handbook of Surveillance Studies* (Routledge 2012) 30.

43 Paul Bischoff, 'The World's Most Surveilled Cities' *Comparitech* (23 May 2023) <https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/> accessed 22 January 2025.

44 Ibid.

45 *Lambert and Others v. France* [2015] ECtHR [GC] 46043/14

46 *Osman v. the United Kingdom* [1998] ECtHR [GC] 23452/94.

47 Margaret Hu, 'Small Data Surveillance v Big Data Cybersurveillance' (2015) 42 Pepp L Rev 773.

48 Irmak Erdoğan, 'Algorithmic Suspicion in the Era of Predictive Policing' in Georg Borges and Christoph Sorge (eds), *Law and Technology in a Global Digital Society* (Springer 2022) 89.

The digital mass surveillance contributes to the protection, defence, and promotion of people against human exploitation and trafficking.[49] States employ internet-based digital methods to identify traffickers.[50] The use of digital technologies, including the tracking of digital traffic or the application of facial recognition systems that evaluate photographic and video evidence within the digital realm, are systematic instruments of digital mass surveillance.[51] Despite the ethical dilemmas and civil rights[52] objections to the effectiveness of these systematic instruments and facial recognition method,[53] from a utilitarian viewpoint, there are potentials to achieve pertaining to crime management and deterrence.[54] The internet, functioning as an instrument of digital mass surveillance, has enabled perpetrators to reach their target population through online profiles.[55] Social media has the potential to greatly enhance the mechanisms of sexual exploitation by employing strategies that coerce individuals into unconsented prostitution. The lover-boy tactic represents a calculated approach used online to manipulate isolated individuals, often focusing on their socioeconomic weaknesses.[56] The digital revolution also has significantly improved labour efficiency and generated opportunities for supply and demand;[57] however, it has also exposed individuals to exploitation through deceptive online job advertisements and social media

49 Saba Demeke, 'A Human Rights-Based Approach for Effective Criminal Justice Response to Human Trafficking' (2024) 9 Intl J Humanitarian Action 1.

50 United Nations Office on Drugs and Crime, 'Using the Power of Technology to Help Victims of Human Trafficking' <https://www.unodc.org/unodc/frontpage/2022/July/using-the-power-of-technology-to-help-victims-of-human-trafficking.html> accessed 01 February 2025.

51 Inter-Agency Coordination Group against Trafficking of Persons, 'Human Trafficking and Technology: Trends, Challenges and Opportunities' <https://icat.un.org/sites/g/files/tmzbdl461/files/human_trafficking_and_technology_trends_challenges_and_opportunities_web.pdf> accessed 01 February 2025.

52 For civil rights debates see: Clare Garvie, Alvaro Bedoya and Jonathan Frankle, *The Perpetual Line-Up: Unregulated Police Face Recognition in America* (Center on Privacy and Technology 2016).

53 Bischoff (n 38).

54 Eric El Piza and others, 'CCTV Surveillance for Crime Prevention: A40-year Systematic Review with Meta-Analysis' (2019) 18(1) Criminology & Public Policy 135; Amanda L. Thomas and others 'The Internationalisation of CCTV Surveillance: Effects on Crime and Implications for Emerging Technologies' (2022) 46(1) International Journal of Comparative and Applied Criminal Justice 81.

55 Europol Operations Directorate, 'The Challenges of Countering Human Trafficking in the Digital Era' (18 October 2020) <https://www.europol.europa.eu/media-press/newsroom/news/challenges-of-countering-human-trafficking-in-digital-era> accessed 12 February 2025.

56 Xavier L'Hoiry, Alessandro Moretti and Georgios A. Antonopoulos, 'Human Trafficking, Sexual Exploitation and Digital Technologies' (2024) 27 Trends in Organized Crime 1.

57 Claudia Roda and Susan Perry, *Human Rights and Digital Technology* (Palgrave 2017) 174.

platforms.[58] Labour exploitation accounts for a significant portion of global human trafficking cases;[59] nevertheless, it is addressed through international soft-law frameworks.[60] Using data gathered from electronic environment—the procurement of digital evidence—facilitates the development of novel legal procedures and practices, enhances the identification of offenders of human exploitation, and strengthens initiatives aimed at safeguarding human rights.[61] The boundless attributes of the digital realm, accessibility at any moment and from any place, offer initiatives for crime prevention with the improved speed and heightened efficiency of reaching to evidences.[62] The implementation of digital mass surveillance and digital evidence streamlines the process of expediting the attainment of justice.[63]

The discussion surrounding digital mass surveillance exceeds mere state institutions; individuals and organisations alike may find themselves entangled in the complex array of risks directed to their personality that accompany this phenomenon. The practice of digital mass surveillance, primarily conducted by private entities for security reasons, raises a term that captures the exploitation of people and their rights within the digital realm—digital colonialism. Digital colonialism reflects historical patterns of human exploitation, emerging through corporations that impose digital dominance over communities, often can be described as the capitalist gaze of digital surveillance.[64] The reliance on digital technologies and the imposition of control without the explicit consent of individuals, coupled with the manipulation of personal data by foreign internet service providers and technology firms, innate transnational human rights concerns.[65] In numerous African nations, the practices of digital mass surveillance,

---

58 Council of Europe, *Online and Technology - Facilitated Trafficking in Human Beings* (Council of Europe 2022) 35.

59 Council of Europe, 'Trafficking for the Purpose of Labour Exploitation: New Online Training Module' (18 November 2021) <https://www.coe.int/en/web/belgrade/-/trafficking-for-the-purpose-of-labour-exploitation-new-online-training-module> accessed 10 March 2025.

60 Letizia Palumbo, *Taking Vulnerabilities to Labour Exploitation Seriously* (Springer, 2024) 34.

61 Isabella Chen and Celeste Tortosa, 'The Use of Digital Evidence in Human Trafficking Investigations' 14 (2020) Anti-Trafficking Review 124.

62 Council of Europe (n 53).

63 Yulia Razmetaeva and Sergiy Razmetaev, 'Justice in the Digital Age: Technological Solutions, Hidden Threats and Enticing Opportunities' (2021) 4(2) Access to Justice in Eastern Europe 104.

64 For details on capitalism and surveillance see: Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Profile 2019).

65 For more detail about digital slavery see: Mick Chisnall, 'Digital Slavery, Time for Abolition?' (2020) 41(5) Policy Studies 488; Michael Kwet, 'Digital Colonialism: US Empire and the New Imperialism in the Global South' (2019) 60(4) Race & Class (2019) 3; Barbara Arneil 'Colonialism versus Imperialism' (2024) 5(1) Political Theory 146.

frequently orchestrated by Chinese enterprises, illustrate a scenario where the oversight of African populations is not conducted by their own people.[66] In the interim, recent research evaluations indicate that the implementation of digital mass surveillance in Kenya does not significantly contribute to a decrease in crime rates.[67] Advocating for liberation from digital suppression is a newly adapted-fundamental human rights imperative. Amid ongoing discourse regarding the exploitation of individuals and the commodification of humanity within the digital realm, one can engage in an exploration of the complex, multifaceted relationships that underpin these phenomena. On one side, there exists digital mass surveillance, a mechanism that can facilitate combating human exploitation; on the other, the digital realm serves as a primary instrument for such exploitation through various multilateral actors and digital colonialism.

Despite the varied national strategies employed by countries, the interplay of digital mass surveillance, preventing crime, human exploitation and trafficking, and human rights reveals a complex duality that highlights both potential benefits and significant risks.[68] The discourse is propelled by this duality, yet it underlines the necessity for a harmonious balance approach in the realms of laws, policies, and practices of digital mass surveillance.

4. Construction of Harmonious Balance

Comprising a diverse array of philosophical, ethical, cultural, and spiritual traditions that have developed over millennia articulates the principles of harmony and balance. The presence of duality is unavoidable; however, the harmonious existence of fluid dualities is of paramount importance in reaching harmony.[69] The dynamic structure of harmony necessitates accepting the coexistence of forces that influence each other and are characterised by variability, resulting in a balance that reflects the essence of reality. To achieve balance with the understanding that the material realm's facets or concerns may display duality when compared to the inherent dignity and of human existence, one must consider the notion of harmonious balance, which encapsulates the paradoxical unity of opposing forces.[70] The interaction of the distinguishing duality through

---

66 Danielle Coleman, 'Digital Colonialism, Digital Colonialism: The 21st Century Scramble for Africa through the Extraction and Control of User Data and the Limitations of Data Protection Laws' 24 (2019) Michigan Journal of Race and Law 417.

67 Njeri Wangari, 'In Africa's First 'Safe City,' Surveillance Reigns'' *Coda Story* (26 November 2024) <https://www.codastory.com/authoritarian-tech/africa-surveillance-china-magnum/> accessed 29 January 2025.

68 Ibid.

69 See Fei Xiaotong, *Globalization and Cultural Self-Awareness* (2015 Springer).

70 For more detail about the idea of the opposing forces and unity see: Tsung-I Dow, 'Harmonious Balance: The Ultimate Phenomenon of Life Experience, a Confucian Attempt and Approach'

dynamic interplay produces a state of balance that harmonises existence and transformation in the world.[71]

The digital mass surveillance and human rights relationship reveals a complex connection that may, in certain circumstances, be characterized by conflicting elements that highlight the inherent imbalance between multifaceted factors. The interplay between digital mass surveillance, the deterrence of crime, the imperative to protect individuals from exploitation, and the commitment to uphold human rights can be characterised as a double-edged sword. Remaining inside the borders of applying the digital mass surveillance, respecting and protecting human rights at the same time has the potential to augment the efficacy and harmonisation questions.

It is neither rational nor suitable to embrace an entirely rejectionist position concerning the opposite ends of the digital mass surveillance and human rights in question. The attainment of a balance, coupled with the policies, represents the most logical strategy for harmonising the evolving landscape shaped by the internet, information communication technologies, and digitalisation. Establishing a compatible harmonious balance have the potential to respect individual rights while simultaneously addressing state interests. Rather than viewing one concept as superseding the other, it is more practical to recognise that the frameworks governing digital mass surveillance and safeguarding human rights can coexist in a balanced harmony. Given the inherently dynamic nature of both phenomena, there exists an opportunity for continuous adaptation that can effectively mitigate their potential divergences.[72]

To achieve a harmonious balance, a precise knowledge of digital mass surveillance must emphasise its critical function in a democracy and should be employed just as a last resort when essential. It is essential to achieve a re-evaluation of personal liberties and surveillance at every stage of the implementation process that remains transparent to avert any potential violations within the notions of legality, necessity, proportionality and transparency thereby ensuring a measured approach with a clear timeframe and objectivity.[73] Mass surveillance must be a method wherein the legal framework is explicitly regulated for all its steps (legality), adopted to fulfil a certain purpose (necessity) by ensuring a proportionality between the purpose and individual rights (proportionality). The

in Anna-Teresa Tymieniecka (eds) *Phenomenology/Ontopoiesis Retrieving Geo-cosmic Horizons of Antiquity. Analecta Husserliana* (Springer, 2011) 645.

71 Ibid.

72 See Mamoona Asghar, et al., 'Visual Surveillance Within the EU General Data Protection Regulation: A Technology Perspective,' (2019) 7 IEEE Access 111709-111726.

73 See David Wright, Michael Friedewald and Raphael Gellert, 'Developing And Testing A Surveillance Impact Assessment Methodology' (2015) 5 (1) International Data Privacy Law 40-53.

mass surveillance must be in maximum openness and accessibility throughout the process (transparency). executed within a reasonable and defined timeframe (timeframe), and wherein the actions and their oversight are grounded in explicit criteria (objectivity).

The interaction between security and human rights must be evaluated at every stage of digital mass surveillance. Importantly, organisations -be they private or governmental- utilising digital mass surveillance for security purposes must embrace a perspective that highlights transparency, accountability, and, most critically, the essential rights of all individuals within a sustainable security framework.[74] Sustainable security advocates for the formulation of a security framework through the attainment of the Sustainable Development Goals (SDGs) 2030 Article 16.[75] The objectives of SDGs 2030 Article 16 necessitate a dedication to safeguarding human rights while tackling security issues, establishing effective, accountable and inclusive institutions at all levels, and secure institutions grounded on the rule of law, and guaranteeing equitable access to justice. A through sustainable security strategy evaluated within the framework of human rights law and practices in alignment with the rule of law to reach a harmonious balance must consistently upheld.[76]

The construction of harmonious balance also rests upon the policies of detection, investigation, and execution.[77] Detection and investigation of internet activities, cryptocurrency transactions, and file sharing, are all vital for uncovering criminal patterns and safeguarding security. The current foremost challenge is the digital evidence. Non-discrimination and right to equality before law standards are upheld to establish veracity of digital data-evidence acquired via digital mass surveillance. The minimum essential guarantees of the right to a fair trial must be implemented in the digital sphere in relation to digital mass surveillance and human rights [78] The standards for the acceptance of digital evidence may include being in compliance with the law, collecting and analysing digital evidence in a manner that is fair, and being necessary for a democratic society. Additional requirements may encompass the capacity to challenge the reliability of digital evidence and particular regulations delineating the conditions

74 Inter-Agency Coordination Group against Trafficking of Persons (n 46).

75 Fiona de Londras, 'Sustainable Security' in Dapo Akande and other (eds) *Human Rights and 21st Century Challenges: Poverty, Conflict, and the Environment* (Oxford 2020) 108.

76 See Finn Kjaerulf and Rodrigo Barahona, 'Preventing Violence And Reinforcing Human Security: A Rights-Based Framework For Top-Down And Bottom-Up Action' Pan American Journal Of Public Health (2010) 27(5) 382-395.

77 Council of Europe (n 53).

78 Radina Stoykova, 'The Right to a Fair Trial as a Conceptual Framework for Digital Evidence Rules in Criminal Investigations' (2023) 49 Computer Law & Security Review 105801 <https://doi.org/10.1016/j.clsr.2023.105801> accessed 22 March 2025.

under which authorities may conduct digital mass surveillance.[79] The execution policy encompasses collaboration and training. Efficiency is imperative for actors to collaborate with independent human rights NGOs that operate within the parameters of their national requirements during the phase of cooperation. Global collaboration ought to be harnessed to advance this essential objective. Appropriate training initiatives, particularly in the realm of digital human rights law, can ensure that all parties remain informed about the evolving landscape of the digital era and grasp the complexities of the digital domain and combating the digital divide,[80] fostering digital literacy,[81] encouraging digital activism.[82] These three concepts are interrelated. Deficiencies stemming from the use of digital technologies—digital divide— and the requisite knowledge and comprehension to interpret and employ digitised content and digital tools—collectively referred to as digital literacy—will produce adverse effects. This condition ultimately jeopardises engagement with civil society or the involvement of political and social events online, which constitutes digital activism.[83] In this regard, the requisite strategy to guarantee accountability in the digital realm must involve the governance of the multi-stakeholder digital framework, in which various entities and stakeholders, such as technology firms, governmental bodies, and individuals, share accountability for digital actions.

In order to establish a harmonious balance in cyberspace, the principles of human rights law, particularly those pertaining to the obligations of states, must be adhered to.[84] States are obligated to uphold human rights also within the digital realm, particularly in relation to their digital sovereignty,[85] and states can

---

79 For details about right to fair trial see: Council of Europe, 'Guide on Article 6 of the European Convention on Human Rights Right to a Fair Trial (Criminal Limb)' (31 December 2019) <https://rm.coe.int/1680304c4e> accessed 22 March 2025.

80 Cynthia K. Sanders and Edward Scanlon, 'The Digital Divide Is a Human Rights Issue: Advancing Social Inclusion Through Social Work Advocacy' (2021) 6(2) Journal of Human Rights and Social Work 130.

81 See Pritika Reddy, Bibhya Sharma, and Kaylash Chaudhary, 'Digital Literacy: A Review of Literature' (2020) 11 International Journal of Technoethics 65-94.

82 See Anne Kaun and Julie Uldam,'Digital Activism: After The Hype' (2018) 20 New Media & Society 2099-2106.

83 Bruce Mutsvairo, 'Dovetailing Desires for Democracy with New ICTS' Potentiality as Platform for Activism' in Bruce Mutsvairo (eds) *Digital Activism in The Social Media Era* (Palgrave 2023) 3.

84 The White House*, International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (The White House 2011) 9.

85 United Nations Human Rights Council, 'Report of the United Nations High Commissioner for Human Rights on the Protection of Human Rights and Fundamental Freedoms While Countering Terrorism UN Doc. A/HRC/13/36' (22 January 2010) <https://documents.un.org/doc/undoc/gen/g10/104/42/pdf/g1010442.pdf> accessed 10 March 2025.

also be deemed responsible for human rights violations that take place beyond their borders.[86] UN accepts that: It would be unconscionable to permit a state to violate human rights, e.g. civil and political rights on another state's territory.[87]

Accountability should be understood in a comprehensive manner and the imperative to uphold human rights transcends conventional governmental entities, as private enterprises increasingly design and oversee technological frameworks.[88] Governments may engage private entities to circumvent their obligations, thus enabling indirect monitoring and acquisition of personal data, which ultimately infringes upon individual rights. Private enterprises frequently engage in partnerships with governmental bodies in the realm of digital mass surveillance initiatives. Social media platforms function as mechanisms for the digital monitoring of individuals, while simultaneously generating revenue for the private entities that manage these platforms and promoting financial inclusion within the context of digital mass surveillance.[89]

Collaborative efforts among institutions and the equitable distribution of responsibilities are crucial for the protection of human rights as articulated in Article 30 of Sustainable Development Goals (SDGs) 2030. The SDGs 2030 pertains to the institutional reforms to be executed, engaging all actors in the processes of implementation and monitoring.[90] Digital rights encompass the creation of multi-stakeholder accountability that aligns with human rights and the sustainability goals of SDGs 2030. According to SDGs 2030, institutional collaboration in the execution of programs for sustainable security necessitates cooperation among all to respect, protect, and fulfil human rights.

In the accountability within the realm of digital mass surveillance both the sovereign powers of the state and the non-state actors-private business

---

86 Vassilis P. Tzevelekos, 'Reconstructing the Effective Control Criteria in Extraterritional Human Rights Breaches: Direct Attribution of Wrongfulness, Due Diligence, and Concurrent Responsibility' 39 (2015) Michigan Journal of International Law 146.

87 *Sergio Euben Lopez Burgos v. Uruguay* [1981] United Nations Human Rights Committee R.12/52, U.N. Doc. Supp. No. 40 (A/36/40).

88 Office of the United Nations High Commissioner for Human Rights, *The Corporate Responsibility to Respect Human Rights: An Interpretive Guide* (UN Human Rights Office 2012) <https://www.ohchr.org/sites/default/files/Documents/Publications/HR.PUB.12.2_En.pdf> accessed 10 March 2025.

89 For details about financial inclusion see: Albérico M. Rosário and Joana Dias, 'Marketing Strategies on Social Media Platforms' (2023) 19(1) International Journal of E-Business Research (IJEBR); Aaron Martin, 'Mobile Money Platform Surveillance' (2019) 17(1/2) Platform Surveillance 213-222.

90 The Danish Institute for Human Rights, 'Human Rights and the 2030 Agenda for Sustainable Development' (2018) <https://www.humanrights.dk/sites/humanrights.dk/files/media/dokumenter/sdg/hr_and_2030_agenda-web_2018.pdf> accessed 12 February 2022.

enterprises must be acknowledging as significant stakeholders.[91] Embracing multi-stakeholder responsibly allows for a legal approach to rectify the accountability gap concerning human rights in the realm of digital mass surveillance. Adopting a contrary perspective and depending solely on state accountability could enable governments to manipulate private business entities as intermediaries, thereby infringing upon and denying individual liberties and rights. The accountability of governments to uphold human rights legislation must be agreeably aligned with the private entities engaged in the digital mass surveillance sector. This alignment aims to foster a collective sense of responsibility and promotes the realization of the SDGs 2030. Additionally, it seeks a harmonious balance for the advancement of the intersection of digital mass surveillance and accountability mechanisms.[92]

The Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law mandates that authorities that implement artificial intelligence (AI)-facilitated digital mass surveillance must consider human rights, democratic principles, the rule of law, and civic engagement.[93] The Convention highlights the importance of preventing illegal and arbitrary practices in AI-driven digital mass surveillance, serving as an important document that sets rules of accountability. The multi-stakeholder approach has been embraced in AI-driven digital mass surveillance, and the existence of the responsibilities of individuals, organisations, and entities has been acknowledged in this context.[94] In the Convention, the principle of transparency refers to the clarity of the AI system's purpose, structure, and actions as well as all of its processes.[95] Additionally, independent oversight is promoted as the presence of mechanisms that have been devised to monitor, evaluate, and guide the activities of AI systems, thereby ensuring a human rights-based oversight.[96]

---

91 For extraterritorial obligations see: Helen McDermott, 'Application of the International Human Rights Law Framework' in Dapo Akande and other (eds) *Human Rights and 21st Century Challenges: Poverty, Conflict, and the Environment* (Oxford 2020) 190.

92 Dorothée Baumann-Pauly and Lilach Trabelsi, 'Complementing Mandatory Human Rights Due Diligence: Using Multi-Stakeholder Initiatives to Define Human Rights Standards' (January 22, 2021) New York University Stern School of Business Research Paper Series <http://dx.doi.org/10.2139/ssrn.3810689> accessed 15 February 2025.

93 Council of Europe, 'Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law" 05.09.2024 <https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence> accessed 23 July 2025, Article 5.

94 Ibid., Article 9.

95 Ibid., Article 8(57).

96 Ibid., Article 8(63).

The Convention also suggests effective, accessible remedies[97] and procedural safeguards[98] for people who have been impacted by human rights violations of the AI-driven digital mass surveillance. The Convention proposes measures to be accepted in the AI-driven digital mass surveillance in case of a threat to human rights, democracy, or the rule of law that may be evaluated as the balance between AI-supported mass digital surveillance and the protection of human rights. [99]

Conclusion

The growing ubiquity of digital mass surveillance, propelled by security concerns, is now associated with the digital exploitation and subjugation, both of which warrant recognition as infringements upon human rights. The digital age necessitates the cultivation of a society that is both globally interconnected and self-sufficient, alongside the establishment of productive partnerships among all participants in information and communication technology to protect digital human rights. The digital landscape and the intrinsic relationship between security and human rights can harness the capabilities of the digital age and engage in strategic actions utilising specific technological instruments. The legal consequences of human rights concerning digital mass surveillance, laden with controversy, oscillate between positive and negative viewpoints.

Choosing a stance or maintaining an unbiased perspective in these discussions can be quite challenging; nevertheless, serves as a framework to elucidate the intricate web of interconnections between benefits and risks across all dimensions of digital infrastructures, including the phenomenon of digital mass surveillance. The principles, such as legality, necessity proportionality and transparency hold significant importance in this context, mandating that surveillance measures must be indispensable for the prevention or investigation of serious crimes. Moreover, digital mass surveillance should be congruent with its designated objectives and the strategies utilised, guaranteeing that personal rights and freedoms are upheld.

Future dialogues will progressively centre on the intricacies of human rights, the expansion of digital mass surveillance, and, importantly, and the implications of digital colonisation, which have attracted considerable scrutiny from both governments and corporate entities. However, maintaining a relevant stance in the digital era by acknowledging that human rights are inherently inalienable and that the nature of colonisation can transform or wane over the course of human history is essential for justice.

A harmonious balanced constructed in towards the digital mass surveillance, human rights, and collaboration is crucial for a framework that alleviates the

97 Ibid., Article 14.

98 Ibid., Article 15.

99 Ibid., Article 16 (112).

uncertainties linked to digitalisation. The harmonious balance requires adopting sustainable security approach, policies of detection, investigation, and execution and multistakeholder accountability that positions both in digital mass surveillance and safeguarding human rights.

References

Akande D and others (eds), *Human Rights and 21st Century Challenges: Poverty, Conflict, and the Environment* (OUP 2020)

Arneil B, 'Colonialism versus Imperialism' (2024) 5 Political Theory 146

Asghar M, Kanwal N, Lee B, Fleury M, Herbst M and Qiao Y, 'Visual Surveillance Within the EU General Data Protection Regulation: A Technology Perspective.' (2019) 7 IEEE Access 111709-111726

Baumann-Pauly D and Trabelsi L, 'Complementing Mandatory Human Rights Due Diligence: Using Multi-Stakeholder Initiatives to Define Human Rights Standards' (New York University Stern School of Business Research Paper Series, 22 January 2021) <http://dx.doi.org/10.2139/ssrn.3810689> accessed 15 February 2025

Bellasio J and others, 'The Future of Cybercrime in Light of Technology Developments' (RAND 2020)

Bentham J, *The Panopticon Writings* (Verso 1995)

Big Brothers and others v. United Kingdom [2021] ECtHR [GC] 58170/13, 62322/14 and 24960/15

Bischoff, P. 'The World's Most Surveilled Cities' Comparitech (23 May 2023) <https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/> accessed 22 January 2025

Bogard W, 'Simulation and Post-Panopticism' in Ball K, Haggerty K and Lyon D (eds), *Routledge Handbook of Surveillance Studies* (Routledge 2012) 30

Bogdan A, 'The Right to Peace in the Context of Contemporary International Reality' (2013) 40 Revista de Stiinte Politice 46

Carpenter v. United States [2017] Supreme Court of United States No. 16–402 <https://cdn.cnn.com/cnn/2018/images/06/22/16-402_h315.pdf> accessed 2 April 2025

Celeste E and Formici G, 'Constitutionalizing Mass Surveillance in the EU: Civil Society Demands, Judicial Activism, and Legislative Inertia' (2024) 25 German LJ 427

Centrum För Rättvisa v Sweden [2016] ECtHR [GC] 35252/08

Chen I and Tortosa C, 'The Use of Digital Evidence in Human Trafficking Investigations' (2020) 14 Anti-Trafficking Review 124

Chisnall M, 'Digital Slavery, Time for Abolition?' (2020) 41 Policy Studies 488

Christakis T and Bouslimani K, 'National Security, Surveillance, and Human Rights' in Geiß R and Melzer N (eds), *The Oxford Handbook of the International Law of Global Security* (OUP 2021) 699

Coleman D, 'Digital Colonialism, Digital Colonialism: The 21st Century Scramble for Africa through the Extraction and Control of User Data and the Limitations of Data Protection Laws' (2019) 24 Michigan Journal of Race and Law 417

Cooley TM, *A Treatise on the Law of Torts, or the Wrongs Which Arise Independent of Contract* (Callaghan & Co 1888) 29

Council of Europe, 'Convention 108+' (2018)

Council of Europe, 'Convention on Cybercrime' (2001)

Council of Europe, 'Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data' <https://rm.coe.int/1680078b37> accessed 2 April 2025

Council of Europe, 'Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law" 05.09.2024 <https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence> accessed 23 July 2025

Council of Europe, 'Guide on Article 6 of the European Convention on Human Rights Right to a Fair Trial (Criminal Limb)' (31 December 2019) <https://rm.coe.int/1680304c4e> accessed 22 March 2025

Council of Europe, 'Trafficking for the Purpose of Labour Exploitation: New Online Training Module' (18 November 2021) <https://www.coe.int/en/web/belgrade/-/trafficking-for-the-purpose-of-labour-exploitation-new-online-training-module> accessed 10 March 2025

Council of Europe, Online and Technology - Facilitated Trafficking in Human Beings (Council of Europe 2022) 35

Danish Institute for Human Rights, 'Human Rights and the 2030 Agenda for Sustainable Development' (2018) <https://www.humanrights.dk/sites/humanrights.dk/files/media/dokumenter/sdg/hr_and_2030_agenda-web_2018.pdf> accessed 12 February 2022

de Londras F, 'Sustainable Security' in Akande D and others (eds), *Human Rights and 21st Century Challenges: Poverty, Conflict, and the Environment* (OUP 2020) 108

de Terwangne C, 'Council of Europe Convention 108+: A Modernised International Treaty for the Protection of Personal Data' (2021) 40 Computer Law & Security Review 105553 <https://www.sciencedirect.com/science/article/abs/pii/S0267364920301023> accessed 10 March 2025

Demeke S, 'A Human Rights-Based Approach for Effective Criminal Justice Response to Human Trafficking' (2024) 9 Intl J Humanitarian Action 1

DiEM25 Communications, 'The EU's Orwellian Agenda: Using Child Protection to Justify Mass Surveillance' (08 October 2024) <https://diem25.org/the-eus-orwellian-agenda-using-child-protection-to-justify-mass-surveillance/> accessed 10 February 2025

Dow T-I, 'Harmonious Balance: The Ultimate Phenomenon of Life Experience, a Confucian Attempt and Approach' in Tymieniecka A-T (ed), *Phenomenology/ Ontopoiesis Retrieving Geo-cosmic Horizons of Antiquity. Analecta Husserliana* (Springer 2011) 645

El Piza E and others, 'CCTV Surveillance for Crime Prevention: A 40-year Systematic Review with Meta-Analysis' (2019) 18 Criminology & Public Policy 135

Erdoğan I, 'Algorithmic Suspicion in the Era of Predictive Policing' in Borges G and Sorge C (eds), *Law and Technology in a Global Digital Society* (Springer 2022) 89

European Commission, 'Proposal for a Regulation of the European Parliament and of the Council Laying Down Rules to Prevent and Combat Child Sexual Abuse' COM (2022) 209 final <https://eur-lex.europa.eu/resource.html?uri=cellar:13e33abf-d209-11ec-a95f-01aa75ed71a1.0001.02/DOC_1&format=PDF> accessed 14 March 2025

European Digital Rights, 'Utopian Dreams, Sobering Reality: The End We Start From In EU's Approach To Technology' (2 April 2025) <https://edri.org/our-work/utopian-dreams-sobering-reality-the-end-we-start-from-in-eus-approach-to-technology/> accessed 2 April 2025

European Digital Rights, 'Why the New Europol Regulation Is A Trojan Horse For Surveillance' (5 March 2025) <https://edri.org/our-work/why-the-new-europol-regulation-is-a-trojan-horse-for-surveillance/ accessed> 2 April 2025

Europol Operations Directorate, 'The Challenges of Countering Human Trafficking in the Digital Era' (18 October 2020) <https://www.europol.europa.eu/media-press/newsroom/news/challenges-of-countering-human-trafficking-in-digital-era> accessed 12 February 2025

Fei X, *Globalization and Cultural Self-Awareness* (Springer 2015)

Galič M, Timan T and Koops B-J, 'Surveillance Theory and Its Implications for Law' in Brownsword R, Scotford E and Yeung K (eds), *Oxford Handbook of the Law and Regulation of Technology* (OUP 2017) 731

Garvie C, Bedoya A and Frankle J, *The Perpetual Line-Up: Unregulated Police Face Recognition in America* (Center on Privacy and Technology 2016)

Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González [2014] ECLI [C]

Hu M, 'Small Data Surveillance v Big Data Cybersurveillance' (2015) 42 Pepp L Rev 773

Inter-Agency Coordination Group against Trafficking of Persons, 'Human Trafficking and Technology: Trends, Challenges and Opportunities' <https://icat.un.org/sites/g/files/tmzbdl461/files/human_trafficking_and_technology_trends_challenges_and_opportunities_web.pdf> accessed 1 February 2025

Ireland v. European Parliament and Council [2009] ECR I-00593

Kaun A and Uldam J,'Digital Activism: After The Hype' (2018) 20 New Media & Society 2099-2106

Kjaerulf F and Barahona R, 'Preventing Violence And Reinforcing Human Security: A Rights-Based Framework For Top-Down And Bottom-Up Action' (2010) 27(5) Pan American Journal Of Public Health 382-395

Kramer IR, 'The Birth of Privacy Law: A Century Since Warren and Brandeis' (1990) 39 Cath U L Rev 703

Kwet M, 'Digital Colonialism: US Empire and the New Imperialism in the Global South' (2019) 60 Race & Class 3

L'Hoiry X, Moretti A and Antonopoulos GA, 'Human Trafficking, Sexual Exploitation and Digital Technologies' (2024) 27 Trends in Organized Crime 1

Lambert and Others v. France [2015] ECtHR [GC] 46043/14

Lyon D, *Surveillance Society: Monitoring Everyday Life* (Open University 2001)

Lyon D, *Surveillance Studies* (Kalkedon 2013)

Lyon D, *The Electronic Eye: The Rise of Surveillance Societies* (Polity 1994)

Martin A, 'Mobile Money Platform Surveillance' (2019) 17 Platform Surveillance 213

Mathew DS, 'Surveillance Society: Panopticon in the Age of Digital Media' *The New Polis* (19 May 2020) <https://thenewpolis.com/2020/05/19/surveillance-society-panopticon-in-the-age-of-digital-media-donna-susan-mathew-part-2/> accessed 10 February 2025

McDermott H, 'Application of the International Human Rights Law Framework' in Akande D and others (eds), *Human Rights and 21st Century Challenges: Poverty, Conflict, and the Environment* (OUP 2020) 190

Mutsvairo B, 'Dovetailing Desires for Democracy with New ICTS' Potentiality as Platform for Activism' in Mutsvairo B (ed), *Digital Activism in The Social Media Era* (Palgrave 2023) 3

Office of the United Nations High Commissioner for Human Rights, The Corporate Responsibility to Respect Human Rights: An Interpretive Guide (UN Human Rights Office 2012) <https://www.ohchr.org/sites/default/files/Documents/Publications/HR.PUB.12.2_En.pdf> accessed 10 March 2025.

Open Letter <https://nce.mpi-sp.org/index.php/s/eqjiKaAw9yYQF87> accessed 10 March 2025

Osman v. the United Kingdom [1998] ECtHR [GC] 23452/94

Palumbo L, *Taking Vulnerabilities to Labour Exploitation Seriously* (Springer 2024) 34

Razmetaeva Y and Razmetaev S, 'Justice in the Digital Age: Technological Solutions, Hidden Threats and Enticing Opportunities' (2021) 4 Access to Justice in Eastern Europe 104.

Reddy P, Sharma B and Chaudhary K, 'Digital Literacy: A Review of Literature' (2020) 11 International Journal of Technoethics 65-94

Roda C and Perry S, *Human Rights and Digital Technology* (Palgrave 2017) 174.

Rojszczak M, *Bulk Surveillance, Democracy and Human Rights Law in Europe: A Comparative Perspective* (Routledge 2025)

Rosário AM and Dias J, 'Marketing Strategies on Social Media Platforms' (2023) 19 Intl J E-Business Research

Sanders CK and Scanlon E, 'The Digital Divide Is a Human Rights Issue: Advancing Social Inclusion Through Social Work Advocacy' (2021) 6 J Human Rights and Social Work 130

Sergio Euben Lopez Burgos v Uruguay [1981] UNHRC R.12/52, UN Doc Supp No 40

Stoykova R, 'The Right to a Fair Trial as a Conceptual Framework for Digital Evidence Rules in Criminal Investigations' (2023) 49 Computer Law & Security Review 105801 <https://doi.org/10.1016/j.clsr.2023.105801> accessed 22 March 2025

Swire P, 'The Second Wave of Global Privacy Protection: Symposium Introduction' (2013) 74 Ohio St LJ 841

Szabó and Vissy v. Hungary [2016] ECtHR [GC] 37138/14

Thomas AL and others, 'The Internationalisation of CCTV Surveillance: Effects on Crime and Implications for Emerging Technologies' (2022) 46 Intl J Comparative and Applied Criminal Justice 81

Tzevelekos VP, 'Reconstructing the Effective Control Criteria in Extraterritorial Human Rights Breaches: Direct Attribution of Wrongfulness, Due Diligence, and Concurrent Responsibility' (2015) 39 Michigan J Intl L 146

United Nations (UN) 'Report of the General Assembly on the Seventy-Third Session: Right to Privacy, UN Doc A/73/4382' (17 October 2018) 4 <https://documents.un.org/doc/undoc/gen/n18/324/46/pdf/n1832446.pdf> accessed 12 March 2025

United Nations Human Rights Council 'Report of the Human Rights Council on Its Thirty-Ninth Session: The Right to Privacy in the Digital Age UN Doc A/HRC/39/29' (3 August 2018) <https://www.ohchr.org/sites/default/files/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/A_HRC_39_29_EN.pdf> 4 accessed 12 March 2025

United Nations Human Rights Council, 'Report of the United Nations High Commissioner for Human Rights on the Protection of Human Rights and Fundamental Freedoms While Countering Terrorism UN Doc. A/HRC/13/36' (22 January 2010) <https://documents.un.org/doc/undoc/gen/g10/104/42/pdf/g1010442.pdf> accessed 10 March 2025

United Nations Office on Drugs and Crime, 'Using the Power of Technology to Help Victims of Human Trafficking' <https://www.unodc.org/unodc/frontpage/2022/July/using-the-power-of-technology-to-help-victims-of-human-trafficking.html> accessed 01 February 2025

Wangari N, 'In Africa's First "Safe City," Surveillance Reigns' *Coda Story* (26 November 2024) <https://www.codastory.com/authoritarian-tech/africa-surveillance-china-magnum/> accessed 29 January 2025

Warren SD and Brandeis LD, 'The Right to Privacy' (1890) 4 Harv L Rev 193

Weber and Saravia v. Germany [2006] ECtHR [GC] 54934/00

White House, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (The White House 2011) 9

Wright D, Friedewald M and Gellert R. "Developing And Testing A Surveillance Impact Assessment Methodology" (2015) 5 (1) International Data Privacy Law 40-53

Ziccardi G, *Resistance, Liberation Technology and Human Rights in the Digital Age* (Springer 2013) 202

Zuboff S, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Profile 2019)