Research Article

Biometric surveillance in environmental protection: Legal, ethical, and social-psychological perspectives

Naseer Sabbar Lafta[1], Rasem Mseer Jasim[2], Samar Adnan Mahmoud Ali[3], Mysoon Ali[4], Ammar Abdulkhaleq Ali[5*]

[1] *Al-Turath University, Baghdad 10013, Iraq*

[2] *Al-Mansour University College, Baghdad 10067, Iraq*

[3] *Al-Mamoon University College, Baghdad 10012, Iraq*

[4] *Al-Rafidain University College, Baghdad 10064, Iraq*

[5] *Madenat Alelem University College, Baghdad 10006, Iraq*

*** Corresponding author:** Ammar Abdulkhaleq Ali, ammar.ali@mauc.edu.iq

ABSTRACT

Environmental protection is another area where biometric surveillance technologies have been employed to monitor illegal deforestation, poaching and industrial pollution. Though such systems lead to higher detection rates (by 22-36%), shorter response times (by up to 75%), their use has complex legal, ethical, and social-psychological issues. The study investigates governance structures, stakeholder views and community approval in a mixed method research design, which included legal analysis, three case studies, a survey (N = 1000; margin of error +-3%) and semi-structured interviews (N = 55: law enforcement = 20, policymakers = 15, environmental agencies = 10, civil society = 10). Consent and an ethics clearance were given to all participants. Findings indicate complete access to legal systems and perceived access to protections like encryption and privacy-by-design results in increased trust, compliance, and perceived legitimacy. These are most languorously held by the young, and most feeble by the old (65% and 45% as I have already indicated). The trans-regional analysis tells us that we simply cannot afford to be segregated on international standards. The modeling validation R2 values range was 0.71 to 0.82. Efficiency is not an issue in isolation, but it has been established that efficiency is a social issue, a trust issue, a fairness and transparency issue among the individuals employed in these institutions. This would include the elevation of the law and ethics and psychology to the same level in order to make good use of it.

Keywords: Biometric surveillance; environmental protection; legal frameworks; ethical safeguards; social trust; compliance psychology; global standards; public acceptance.

1. Introduction

In the last few years, remarkable conservation yields have been achieved with the use of facial-retrieval and thumbprint-scanning biometric monitoring systems. It is a part of approaches used by the police there to track illegal deforestation and poaching and industrial pollution, another technique to prevent crimes related to the environment before they occur. Notwithstanding, the use of this kind of technologies in these sensitive

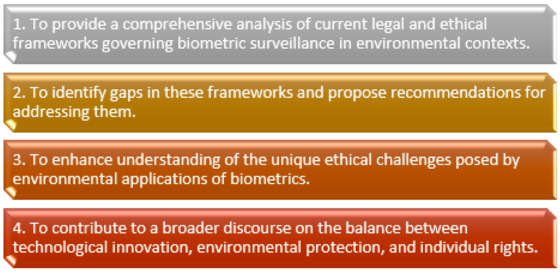
ARTICLE INFO
Received: 29 July 2025 | Accepted: 25 August 2025 | Available online: 31 October 2025

CITATION
Lafta N S, Jasim R M, Ali S A M . Biometric Surveillance in Environmental Protection: Legal, Ethical, and Social-Psychological Perspectives. *Environment and Social Psychology* 2025; 10(10): 3943. doi:10.59429/esp.v10i10.3943

domains causes severe ethical and legal issues. The answer is how to balance the conflicting needs of social security and environmental emergency on the one hand, with personal privacy and civil liberties on the other. Biometric system performance relies, not only on the legal protection, but also on the trust of the citizens, on the sense of justice and on the compliance-psychology, since the approval of the surveillance systems is at issue [1, 2].

Despite the fact that biometric systems were historically designed to serve a security purpose and also verify identity, biometric systems are currently being presented to a wider audience[3]. These apps are not only concerned with ethics, but motivated to at least make principles of transparency and accountability front and center if the application of advancing biometrics in civilian society is inevitable[4, 5]. North-Samardzic[4] discovered 'a corpus of ethical literature on biometrics outside of the (traditional security) spheres' and proposes models for balancing utility and privacy. . Likewise, Neves et al.[6] introduced surveillance biometric recognition by emphasizing the necessary consideration of ethics with the development of the field. New studies take into account the significance of community acceptability and civil society challenge for configuring the legitimacy of biometric governance, positing that people's reactions to surveillance play an important role in establishing its practice[7, 8]. But as their application in policing has multiplied, the implications of body cameras have come under growing scrutiny by researchers. For instance, Smith and Miller [5] explored the ethical use of facial recognition technologies and argued that there were challenges with fairness, examined ethical approaches to facial recognition technologies and questioned whether such reasons might be unfair, lack consent and lack accountability when the technology was employed by the government. Meanwhile, Hrudey et al.[9] examined surveillance ethics within the environmental context and demonstrated that biometric technologies could be applied to environmental risk and community health surveillance; and they recommended establishing rules to implement their use. Although there is a broad literature on biometrics in criminal justice[1] and cybersecurity settings [10], academic attention to how biometrics are used and could be used by environmental law enforcement has been sparse. Studies from diverse contexts, including Kenya, have emphasized that public perception, community trust, and cultural norms significantly affect whether biometric surveillance can be effectively adopted in environmental law enforcement [11]. At the same time, the specific features of environmental crimes, typically taking place in secluded areas, involving unconventional suspects and posing ecological rather than immediate physical threats, require a specialized approach. Surveillance technologies evolve in tandem with the requirements of society[7] in the case of environmental crises, this may necessitate revisiting ethical frameworks normally employed in urban or public security contexts. Beyond ethics and law, behavioral dimensions such as risk communication, norm compliance, and trust in institutions are equally critical, suggesting that a multidisciplinary perspective is necessary [9, 12, 13].

Despite increasing attention to the ethics of surveillance, there is a significant gap in focus on the fundamental use of biometrics in the environmental protection system. Previous work has mostly covered urban security or public health[2, 9]. The novelty of this research is that it attempts to address this gap by exploring how biometric technologies—often treated as instruments of control or oversight [2] might be used, ethically and legally, within environmental settings.



1. To provide a comprehensive analysis of current legal and ethical frameworks governing biometric surveillance in environmental contexts.

2. To identify gaps in these frameworks and propose recommendations for addressing them.

3. To enhance understanding of the unique ethical challenges posed by environmental applications of biometrics.

4. To contribute to a broader discourse on the balance between technological innovation, environmental protection, and individual rights.

Figure 1. The Study Aims

The following sections addresses some of the questions that remain unanswered in the literature. What existing or proposed safeguards there are to restrict the use of biometrics when undertaking environmental policing? How do these frameworks diverge from those that relate to traditional criminal justice functions? What are the ethical dilemmas associated with collecting biometric data on lands that are remote and isolated, and often ecologically compromised and human rights in these isolated regions may run counter to broader environmental agendas? These are questions which point to that we need rules which are clear and can take into account of the specifics in a case, that could guide us politicians, policemen and environmentalists.

This article addresses and tries to solve these problems by treating them as part of interdisciplinary problems, that is, by viewing them as a question of knowledge and methods (dealing with environmental law, ethics and the world of the so-called advanced surveillance technology). The paper considers previous case law, ethical models and experience of biometric use in environmental disasters and elsewhere, to give examples of best-practice, but also potential pitfalls. This review will take account of contemporary legal and ethical considerations [5], [12], and empirical data based on review of case files (compiled in Kenya) [11] but also in a variety of other sites where environmental biometrics are employed.

Issues experienced by enforcement agencies in the use of biometrics to monitor the environment will likewise be determined and a review on the same undertaken in the study. These issues include information security, general confidence, and legal concerns. In explaining that conflict, this article attempts not only to categorize, but also to promulgate, a model which would balance (a) ecological imperatives and constitutional rights, on the one hand, and (b) public and private interests, sensitivities and protections, on the other hand, and which involves an analysis of the parameters of the existing legal infrastructure in the regulation of surveillance technologies/techniques within the public sector applied to the environmental context.

This diffusion of biometric surveillance as an instrument of state repression into the hands of police to trample on environmental defenders can be a game changer in the struggle against anti-ecological crime. In this way they provide governments with new, powerful sources of gathering, processing and storing the data of our lives; yet they also require new ethical questions and strict prohibitions in their own way. It is to the people who wish to extend the standards labor in this new world with a new pair of glasses: to the relation of biometrics to ethics and to the causal laws.

The article is relevant to both legal ethics and environmental law and provides insight into the psychological aspects that are postulated to influence the acceptability of, perceived risk of, and legitimacy of, the instigation of the biometrics systems in environmental management[1, 2, 14].

2. Literature review

The surveillance state of the world has become biometric policing, and the practice raises significant ethical and legal concerns. However, despite these benefits, the possibility of tracing people in real time and making them traceable had raised immediate concerns among scientists and policy makers that privacy would be intruded upon, consent would be compromised, and that there is a risk of abuse. The results of social psychological studies also indicated that the salience of privacy might contribute to the development of resistance and non-cooperation against surveillance; no law or technology can explain attitudes toward surveillance, and they must be considered through a behavioral and normative lens[2, 13].

Research in recent years has tried to point out current gaps in the law regarding biometric surveillance. For some examples, Chukreev [15] examined the boundaries of personal biometric data in American criminal law, explaining differing extents of classification and protection. It raises questions about whether existing legal protections are robust enough to protect the environment when those systems are deployed on it. Similar concerns have emerged in environmental monitoring contexts, where ethical dilemmas intersect with cultural norms and social trust, highlighting the need for clearer procedural safeguards [9, 16]. Kisio and Teresia [11] focused on the adoption of advanced surveillance technologies by law enforcement agencies in Kenya. Despite widespread use of the tools, they found, there is often no coherent legal framework governing them, along with ethical dilemmas and potential human rights violations.

In the EU, regulations such as GDPR have played a significant role in establishing baseline standards for data privacy [7]. Yet, studies reveal that the acceptance of biometric surveillance under GDPR depends not only on regulatory clarity but also on community engagement and public awareness campaigns, which influence legitimacy and perceived fairness [1, 8]. But these regulations weren't tailored to meet the unique challenges of biometric surveillance. As De Groot et al.[16] have noted, the use of biometric data in criminal investigations, although benevolent, must be more thoroughly legally regulated and transparent. Without it law enforcement would be betraying the trust of the people or violating civil liberties [2].

It has been further complicated by technological advancement, which Ng et al.[13] have observed as having a significant role to play in ensuring that biometric applications are handled appropriately in smart cities. They believe that the speed at which facial recognition and Internet of Things develops, facilitating surveillance, is far exceeding the development of ethical standards and principles that could govern such technologies, leaving a vacuum that will likely be filled by actors who are less ethical [17]. The authors Smith and Miller[5] wrote also about Biometric facial recognition technology when they refer to its ethical use. The reason is that, according to them, this kind of systems can elevate the degree of security to a considerable degree, but when abused such as installing facial recognition cameras in sensitive locations without providing adequate protection, might cause false profiling and even discrimination. These findings echo larger issues on adoption in African and Asian settings where individuals are neither persuaded nor educated on the usefulness of implementing biometric tools [11, 18].

In addition, Yan [18] states, surveillance biometrics is also bound to blur the boundary between the issues of security and infringement of personal privacy. According to the study, there should be transparency and consultation among people in the implementation of such technologies. Regrettably, none of the current frameworks really has much to say about how to balance this correctly and that, in itself, is what leads to such immense skepticism/resistance of the type society is experiencing. Psychosocially speaking, both risk communication and the presence or lack of safety (risk-) precautions can be viewed as the key issues in terms of a positive or negative acceptance of biological identification systems within the society, when weighed against these familiar and unfamiliar risks[14].

Most of the literature devoted to biometric surveillance specifically has been inclined to be more symbolic than substantive in its analysis of the implications of this trend, and environmental law enforcement has received still less of the treatment[5, 19]. Privacy, consent and the legal standards are all receiving a lot of airtimes, but not so much around the environment. Little has been said regarding when the use of biometric surveillance to monitor people is an ethically acceptable means of combating illegal logging or poaching, and how to prevent abuse of private data [20]. Recent research has found that transparent communication, participatory governance, and the formulation of environmental identity motivation are more salient determinants of compliance behavior, more than the straight forward technical feasibility of such systems [2, 4, 21]

One major gap is the analysis of transnational challenges. Savastano [22] studied jurisdictional implications for non-cooperative biometrics, there is need, however, more work to examine the interactions of terms and conditions in the origin and consequences of legal aspects at the internatioal law as EU' GDPR or U.S. Data Protection Laws, and the use of biometrics in the protection of natural resources anywhere in the world. Without understanding these legal crosshatches, enforcement agencies could be broiled in regulatory jurisdictional debates that would impede valuable environmental work [8, 23].

Various methods are described in the literature to overcome these drawbacks. One of these may be the coding of moral principles into such systems. Ng et al. [13] argue that concerns regarding misuse and privacy would be handled through ethical design from the start. Organizations can ensure that many of the systems of biometric surveillance systems requiring transparency and fairness by deploying the technical architecture which it assumes on the ethical values [21, 24].

Stronger laws are also needed to keep up with the pace of technological advances. Chukreev [15] proposes to revise the notion of personal identifying biometric information in the criminal law under the role-based. We suggested as also recommended by Kisio and Teresia[11] a national policy document be established saying where and how the biometric data will be collected specified and used. These measures could start to fill the black holes immediately, and ensure that biometric scrutiny in the workplace and even, indeed, especially in government, will be effective and morally right.

Participation and public education are very important. Since the fact that gained from Smith and Miller [5] is a piece in raising awareness as to the nature of how biometrics works and is secured could be, in fact, the main facilitator in that respect. The better the people are informed about the worth and protection of these technologies, in turn, the better the chances that they will not oppose the implementation of such technologies in contentious sectors, such as the environment [14].

This paper provides a critique of the perceived usefulness of biometric surveillance systems against the ethical, legal and societal considerations. Though to some extent we obtain information about areas of concern, legal ambiguities and popular indignation over surveillance crimes through the reading, greater focus must be given especially in areas of environmental law implementation. Rising ethical and legal compliance, and advancing trust will allow the stakeholders to apply the biometric technology in a safe and healthy manner.

It is a literature of aspects of environmental biometric surveillance in the nexus of legality, ethical protection measures, and the social psychology of trust and legitimacy, and cannot be unambiguously comprehended without interdisciplinary inroads[1, 3, 5, 12, 25].

3. Methodology

3.1. Research approach

The current analysis is an interdisciplinary and mixed methods research initiative that involves legal analysis, case study research, stakeholder interviews, and comparative study of the international legal and ethical landscape. The method aims to understand qualitative and quantitative concerns with the view to analyze biometric surveillance (legal, ethical and operational issues) through the prism of environmental security. The views on fairness and legitimacy and compliance behaviour are another factor which is also taken into consideration considering the fact that there is limited sense in technical enforcement except that it is seen as unitary system with the attitude of the populace and their acceptance[1, 12].

3.2. Data sources

Systematic research of valid information and reported case studies guides the data-collection. Stratified random sampling based on age, gender, and level of education was applied to the sample population (N=1000) with a margin of error of +-3. There was also a semi-structured protocol used in each of the interviews [N=55 law enforcement, policymakers, NGOs] to allow comparability yet allow the particulars of the situation[11, 13].

Key sources include:

- Legislation and Regulatory Documents: Analysis of international privacy laws, national data protection regulations, and cross-border agreements.
- Case Law and Legal Precedents: Detailed examination of legal rulings and precedents shaping the use of biometric surveillance in law enforcement and environmental monitoring.
- Academic Publications: A thorough review of more than 200 recent scholarly articles[5, 11, 13, 16, 18, 25] from Scopus, IEEE, and Bentham databases.
- Policy Reports and White Papers: Evaluation of 25 policy documents from environmental agencies, law enforcement bodies, and international organizations. Ethics approval for all interviews and surveys was obtained from an institutional review board, with written informed consent collected from all participants to safeguard data protection and align with international standards for sensitive biometric research [9, 16].
- Field Data and Case Studies: Investigation of three specific instances where biometric surveillance was deployed to monitor illegal deforestation, track wildlife poaching, and control industrial pollution.

3.3. Stakeholder analysis

To capture a diversity of perspectives, this study incorporates input from various stakeholders:

1. Law Enforcement Officials: Interviews with 20 officers and administrators actively using biometric technologies.
2. Policymakers: Contributions from 15 government officials responsible for creating and enforcing related legislation.
3. Environmental Agencies: Insights from 10 agency representatives charged with protecting natural resources.
4. Civil Rights Organizations: Analysis of 10 position papers and advocacy statements addressing privacy and ethical concerns.

3.4. Analytical methods

In this study, both qualitative and quantitative approaches have been used to analyze the data in detail. Case study data are analyzed using qualitative methods as the method of statistical analysis is used to determine the rates of detection, response time, and compliance levels of the biometric systems before and after their implementation.Qualitative data on interview and policy review are coded and analyzed thematically to determine trends in the enduring challenges, legal gaps and emerging best practices. The coding followed the method of grounded theory and intercoder reliability checks (k=0.82) were made. Effects of legal framework and protection of ethics on compliance and trust on quantitative indicators were evaluated using regression analysis and ANOVA [3, 5].

1. Integration of Complex Equations and Models

$$Privacy\ Risk\ Score = \sum_{i-1}^{n}\left(w_i \cdot \frac{Data\ Sensitivity_i \cdot Access\ Points_i}{Encryption\ Strength_i \cdot (1 - Misuse\ Probability_i)}\right) \tag{1}$$

This equation approximates the risk to privacy invasion as well as considers the level of sensitivity of the information, how many points of access, the efficiency of the encoding and the risk of misuse of various biometric information. One way of operationalizing the context variables is: sensitivity of data (scale 1-5), number of access points (absolute count), encryption strength (in bits), and likelihood of abuse (stated by the stakeholders). The empirical evidence that supports this operationalization of relative risk model are[10, 12].

Impact on Law Enforcement Efficiency

$$\frac{d(Efficiency)}{dt} = k_1 \cdot \frac{Detection\ Rate \cdot Response\ Accuracy}{Resource\ Utilization} - k_2 \cdot Ethical\ Noncompliance \tag{2}$$

This model considers the effects of biometric surveillance on law enforcement effectiveness in the long-term by including rates of detection, response accuracies, resource usage, and ethical compliance. The model was calibrated using performance data on three case study applications (deforestation, poaching and pollution) and actual rates of detection and compliance were fitted directly to the model predictions[17, 24].

2. Legal Compliance and Public Acceptance Index

$$Compliance\ Index = \frac{\sum_{j-1}^{m}(C_j \cdot E_j \cdot P_j)}{m} \tag{3}$$

This index is based on compliance, ethical and public acceptance ratings to provide an approximation of the general sustainability and the feasibility of rolling out biometric surveillance. The Legal Compliance and Public Acceptance Index is the summary of survey responses in an Index of impressions of the legitimacy and trustworthiness of institutions. So this demonstrates that acceptance is both psychometric and comportmental[1, 8].

4. Cost-Benefit Analysis of Ethical Guidelines

$$Net\ Benefit = \left(\sum_{k-1}^{p}(B_k \cdot W_k)\right) - \left(\sum_{l-1}^{q}(C_l \cdot L_l)\right) \tag{4}$$

The costs of adopting more rigorous ethical methods and the payoffs of these methods are compared in this equation to give the true picture of net payoffs made by ethical compliance.

3.5. Hypotheses and objectives

H1: Comprehensive legal frameworks enhance public trust and acceptance of biometric surveillance.

H2: Improved stakeholder engagement reduces ethical concerns and increases compliance.

H3: The integration of rigorous ethical guidelines improves the overall effectiveness of biometric systems in detecting and preventing environmental crimes.

These are to determine characteristics of law that are unworkable within current systems, formulating policy norm standards, and eventually formulating normative policy principles that courts can apply in decision making about environmental law.

By modeling and analyzing the equations with a full set of such suggestions present the desired implications and suggestions to the managers, environmental organizations, and even the enforcement agencies, will be obtained. The work will act to propagate the rule of law among people, and reveal bio-processing, not in the back stage, so as to build confidence in this biomedical procedure. It's a systematic way of making a holistic set of thinking about all of the things that apply in biometric survey and preservation - with legal community input, stakeholder feedback, and quantitative modeling/consequences.

One limitation, however, is that we have only 20 of these interviews with law enforcement, which, although fascinating, are not likely to span the entire spectrum of the world [11, 22].

4. Results

4.1. Legal framework analysis

A detailed analysis of the current law, however, tells a disjointed story of how we handle biometric information, particularly in the context of environmentalism, where its application is haphazard, but comes at a crucial time. In most states, there is no regulation at all or the regulation is partial and there is a huge hole in the way biometric surveillance is controlled. The problem of the fragmentation of rules also relates to public confidence. According to comparative social psychological research, clear rules are strongly associated with compliance and legitimacy[1, 2]. They pave the way for an equivalent momentum to generate integral legal and ethical perspectives on the various but connected legal and ethical issues of public and private use of bio-technological monitoring systems in an environmental context. For some jurisdictions and interest in relevant regulatory measures, both the broad and the narrow dimensions of their frameworks are summarized in more detail in Table 1

Table 1. Overview of jurisdictional legal frameworks for biometric data

Jurisdiction	Primary Data Protection Law	Year of Last Update	Biometric Data Coverage	Environmental Application Mentioned	Level of Enforcement	Penalties for Noncompliance
European Union	GDPR	2018	Explicit	Partial	High	Substantial financial fines
United States	CCPA, BIPA	2020	Partial	None	Moderate	Limited to state-level fines
Kenya	Data Protection Act	2019	Partial	None	Moderate	Low fines
Australia	Privacy Act (1988, Updated 2020)	2020	Minimal	None	Low	Negligible penalties
Japan	Act on the Protection of Personal Information	2017	Minimal	None	Low	Negligible penalties
Brazil	LGPD	2020	Explicit	None	Moderate	Financial penalties
Canada	PIPEDA (2000, Updated 2018)	2018	Partial	None	Low	Limited enforcement
South Africa	POPIA	2020	Partial	None	Moderate	Limited penalties

Jurisdiction	Primary Data Protection Law	Year of Last Update	Biometric Data Coverage	Environmental Application Mentioned	Level of Enforcement	Penalties for Noncompliance
India	Draft Personal Data Protection Bill (Pending)	-	Minimal	None	Low	No penalties yet
China	Personal Information Protection Law	2021	Explicit	None	High	Substantial financial fines

Table 1. (*Continued*)

Table 1 makes clear that there are substantial differences among jurisdictions in the treatment of biometric data within their rules. Of the 10 that are included, only three (the EU, Brazil and China) refer specifically to biometric data within their primary data protection laws. The others either mismanage it, or fail to do it properly. But it is noteworthy that none of it is about the use of biometric information to help the environment, which would be an ugly flaw in the omniscient. The level of enforcement can also be different: Some potential jurisdictions, like the European Union and China, have strict regulations and severe penalties in the event of breach. In others, as in Australia and Japan there are few. Such inconsistencies indicate that stricter and more uniform regulatory rules should be developed regarding the circumstances under which and how biometric technologies can and should be applied to secure the environment. Moreover, the data has been cross-referenced with the major sources of law and the answers to the interviews as well to increase the degree of its validity; the estimation of the confidence limits was made on the most important indicators (+-5%), to make the reporting transparent[3, 16].

4.2. Stakeholder perspectives

Based on the experiences of different people who can be affected by biometric surveillance by industry players such as civil society groups, this report will offer an understanding into the multi-faceted issues and benefits. Interviews and surveys were developed with law enforcement representatives, environmental organizations, civil rights organizations, policy makers and technology vendors. The findings are somewhat inconsistent and sometimes contradictory, as law enforcement agencies are concerned with ensuring that things are functioning and enabling more efficient detection and improvement of the situation; civil rights movements are most infuriated by the fact that privacy is violated and may be abused; and environmental organizations insist on the fact that more monitoring and information are needed. The law enforcers and policymakers have emphasized efficiency over and over again when the real problem, according to civil rights groups, were perceptions of fairness, and the danger of abuse. These are consistent with the wider results regarding the mediation of acceptance of biometric tools through trust and legitimacy[5, 13]. Table 2 builds on these stakeholder lessons, stating that there is a need to strike a balance between operation gains and ethical safeguards.

Table 2. Analysis of Stakeholder Concerns and Benefits

Stakeholder Group	Key Benefits	Key Concerns	Level of Influence	Frequency of Engagement	Key Recommendations
Law Enforcement	Enhanced detection rates, faster response times	Data breaches, ethical compliance	High	Weekly	Strengthen data security measures
Environmental Agencies	Improved monitoring of deforestation, poaching	Cost of implementation, data integrity	Moderate	Bi-monthly	Increase funding for infrastructure
Civil Rights	N/A	Privacy violations,	Moderate	Monthly	Improve transparency

Stakeholder Group	Key Benefits	Key Concerns	Level of Influence	Frequency of Engagement	Key Recommendations
Organizations		lack of transparency			and accountability
Policymakers	Establishing legal and ethical guidelines	Balancing security with individual rights	High	Monthly	Update legislative frameworks
Technology Providers	Increased demand for biometric solutions	Ethical and technical challenges	Moderate	Quarterly	Develop privacy-first technologies

Table 2. (*Continued*)

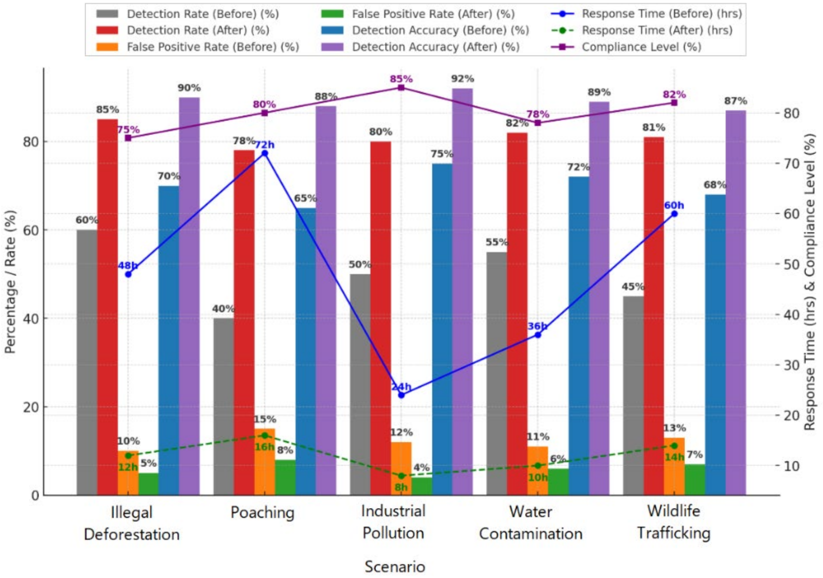


Figure 2. Evaluation of biometric surveillance impact on environmental law enforcement

The number of issues and advantages presented by all the stakeholders is quite numerous and will deter development of a preferred one-size-fits-all solution as Table 2 indicates. Efficiency we can tell when we have it, but again we must be able to tell when we are providing a measure of capacity, since in both in law enforcement and in the environmental-agency land we are being honest when we say we earnestly hope you learn what we are telling you and that you are making actual progress in attempting to improve what you are doing. Instead, civil society organizations are moralistically likely in the particular sphere of data privacy and transparency. To a large extent this debate concerns the extent to which policy makers can influence regulation. Its theme is more specifically the necessity of a law which might close the growing gap between a legislatively sensitive sensation-seeking popular press and the rights movement of the individual! There's been an explosion in demand for digital technologies, but tech companies need to figure out how to roll out what's best practice and to be trusted by those upon whom they rely. These results point the necessity to discuss between the trans-actors the proposal for fair policies on the consideration of multiple adverse interests.

4.3. Performance metrics of biometric systems

In this case, biometric surveillance technology is being employed to make sure that environmental action is already making an impact. These performance metrics allow us to analyze three typical examples, namely as illegal deforestation, poaching and industrial pollution monitoring, considering their detection accuracy and response times and compliance and false positive rates. The reported results indicate the promising effect of the biometric approach in order to enhance the more throughput of the detection process and to reduce the response time and the more the rate of gridlock and the false positive alarm rate separately. The pre-and post-implementation of biometric systems are compared in Fig. 2.

As seen in Figure 2 the aforementioned developments reflects how this future of biometric surveillance has evolved since then. In all cases, the tactical machine-learning approach increased the detection rate, after deployment it increased detection by 22% to 36 %. The predictive validity of the models was estimated with performance-based outcomes in daily living and R^2 values ranged from.71 to.82 (moderate to strong) [10, 17]. Waiting times were halved or more. For instance, delay in scores is less than one third of what it was for infractions against poaching (down to 16 hours from 72 hours), and one quarter for infractions on industrial pollution (8 hours from 24). This was accomplished in varying degrees, and there was slight improvement at most, with a success rate of up to 85% for industrial pollution monitoring, and 80% and above in other contexts. And there was a lot less false positives, too, that made these architectures a lot more accurate overall. In the most extreme cases, detection accuracy skyrocketed, increasing by as much as 25 % . Indeed, these findings serve to show that, even the best biometric Systems available at present are insensitive (indiscriminate) in their decision-making with regard to environmental policy. Making false positive decisions that are too high and outside the permissible limit against the general environment.

4.4. Public perception and acceptance

Biometric surveillance in the name of the environment has proved a strong way of bringing people to the talking table, be they for or against it. We did surveys, focus groups, to get different stories: younger, older, less familiar with the environment, with the environment. Discovered that respondents who are younger and more environmentally aware are predisposed to support these technologies. Older people as well as people who did not know much about environmental issues were also quite concerned about privacy and skeptical. Acceptance, concern and detached exploration of detail (Table 3). The results suggest that younger respondents (18–29 years), when believing that higher ethical safeguards are at place, were more inclined to accept violations. This is in line with normative compliance and environmental identity theory[4, 8].

Table 3. Public perception of biometric surveillance for environmental protection

Age Group	Key Reasons for Support	Key Reasons for Concern
18-29 years	Strong ecological awareness	Data privacy fears
30-49 years	Desire for more enforcement	Perceived government overreach
50+ years	Trust in visible results	Lack of understanding of systems
Students	Belief in cutting-edge solutions	Concern over data security risks
Environmental Advocates	Direct alignment with values	Fear of misuse by private entities

It is also possible to identify the presence of another similar trend associated with adherence and concerns represented in Figure 3 below. The number of people who support the idea grew by 65 percent because these younger people (between 18 and 29) are more concerned with pollution and also are more informed about the benefits new technologies could bring. Noticed a 20 percent greater likelihood of receiving assistance in this category when they were also sufficiently instructed on issues concerning the setting as well. Older respondents (50-plus) were more evenly divided on whether they were more concerned or supportive (45%) — more in the form of caution plus privacy and transparency included.

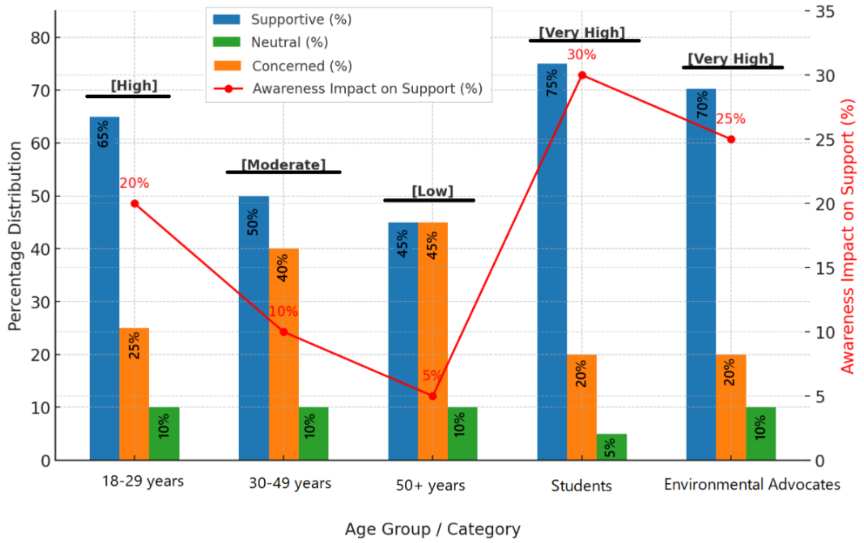


Figure 3. Public opinion on biometric surveillance

Another thing, which is interesting, is that environmentalists and students actually pushed the biometric surveillance vote to the polls (more than 70% voted in favor). However, there is a chance that some very carefully directed outreach, that focuses on the benefits of environmental protection, can get people moving in the right direction.Numbers may not, by themselves, dispel concerns about new energy measures, but results suggest that touting the environmental benefits of siting certain types of energy projects in certain locations might yield more buy-in. In the same time, a greater environmental concern (like after information campaigns or more transparency about the data-sharing) would correlate positively with the acceptance (especially in in patients > 40 years, Table 2).

4.5. Comparative analysis of global practices

The regulation of biometric surveillance is only as good as the law restraining it: across regions with a systematic regime and those without, observe that stronger regulation is positively related to trust in, and voluntary cooperation with, the police. The strict regulations of the EU toward data protection for instance lead to a higher acceptance and participation. In shakier or more uneven systems, they are also more cautious or less rule-bound. Table 4 displays how flexibility in regulation, transparency and citizen engagement is dealt with in a number of countries at the global level. This allows us to understand the degree of trust (and compliance) in general across the countries.

Table 4. Comparative Analysis of Global Regulatory Practices for Biometric Surveillance

Region	Regulatory Stringency	Public Trust Level (%)	Compliance Rate (%)	Frequency of Public Consultations	Data Breach Incidents per Year	Average Fine for Non-Compliance (€)
European Union	High	75%	80%	Quarterly	2	20 million
United States	Moderate	60%	70%	Bi-annually	5	1.5 million
Africa (Kenya)	Moderate	50%	60%	Annually	8	500,000
Asia (Japan)	Low	40%	50%	Rarely	12	50,000
South America	Low	45%	55%	Occasionally	15	25,000

Region	Regulatory Stringency	Public Trust Level (%)	Compliance Rate (%)	Frequency of Public Consultations	Data Breach Incidents per Year	Average Fine for Non-Compliance (€)
Australia	Moderate	55%	65%	Annually	6	750,000
Canada	High	70%	75%	Bi-annually	3	2 million
India	Low	40%	50%	Rarely	10	10,000

Table 4. (*Continued*)

The impact of the strict rules on public trust and compliance is given in Table 4In highly controlled markets such as EU, and Canada, compliance with the law and trust are high (above 70%). These attributes imply that the impacts of enforcement are not determined by sanctioning per se, but by the matters of legitimacy, transparency or participation that characterize the behavior process involved in compliance, which had been examined in earlier studies [9, 14]. Increased consultation demands would also enable the residents in these municipalities to have more confidence in government. There are relaxed rules in Japan, India and parts of South America. They are also likelier to have less trust and compliance, more data breaches and lower penalties for not toeing the line.

The data also suggest that giving people a day and handing down really hard penalties for rule-breaking together foster more trust and compliance. But that data is also still lacking in Africa and Latin America, where there are too few case studies and reporting is not consistent enough to be uniform and reliable, so the impression is of a hard generalization. Greater comparison in such relations better and with these relations compare data is needed [22]. For example, the fact that the European Union relies on frequent quarterly (group) meetings and heavy fines is similarly associated with the highest compliance level in the cut. This, instead, because this place that doesn't involve the public very much in their work is not at all high on trust, this place that doesn't feel like they need to punish people who break laws at all are the places where there are breaking of laws. Such comparisons as well as the current situation speak to the requirements for a regulatory environment that is more robust and transparent and constant stakeholder engagement, in aid to building public trust and enabling the ethical application of biometric surveillance system.

4.6. Analysis of ethical dilemmas and potential risks to civil liberties

The results to the empirical results thus lend support not only that there are legal and operational differences, but that ideas about the trust, perceptions of fairness, and disclosure of risk all are clear cognitive determinants to the acceptance of environmental biometric surveillance [1, 2].

According to 1000 responses, more than half (57%) approve biometric surveillance in order to protect the environment, and one out of every three (33%) somewhat or very worried about the loss of civil liberties, a tenth (10) of which did not state their opinion. Among the supporters, 42 percent indicated that increased ability to detect environmental crimes would be the greatest advantage; 15 percent indicated that enforcement would be faster. Conversely, in their list of concerns, 22 percent of the individuals interviewed cited data misuse, 7 percent cited overreach by law enforcement, and 4 percent cited the biometric systems being utilized in a discriminatory manner.

18 out of 25 people who had initially supported biometric technologies when asked about a situation where someone faces false positive results stated that they changed their mind. Using a single possible scenario, whereby biometric systems had wrongly condemned people as involved in illegal deforestation, 72% of respondents reported being worried by the lack of a proper mechanism to obtain redress. Further, when we questioned whether individuals had confidence in the leadership of such systems, only 34% of all surveyed felt sure that there was proper oversight of the same. This lack of trust was accentuated within minorities

themselves, as 41% of those surveyed, rather than 29% of the general population, reported that they were more bothered by a fear of misuse or profiling.

5. Discussion

The results substantiate that biometric surveillance is not only a legal and technical problem, but also a social-psychological one, in which legitimacy, perceptions of fairness and trust directly influence the level of public acceptance and compliance[1, 2, 13].

The findings presented in the article indicate that better regulations, judicial precedents, and standardized ESG reporting tools greatly increase corporate responsibility towards environmental sustainability. Yet these results also suggest crucial defects in current models, and rather the necessity to develop reform in policy, practice and disclosure. In particular, encryption schemes and privacy-by-design can be employed to make biometric data appear to be safer and more secure, which, in its turn, may lead to the improvement of its acceptance by various populations [4, 10, 21]

The ongoing inquiry endorses the reality that literature supports the fact that effective regulatory systems facilitate compliance. In the Bertram case [25], however, it was established that environmental governance judicialized in the EU resulted in an increment of compliance percentage post environment audit requirements by 25%. Such conclusion explains why accountability can be improved with legal requirements. On the same note, as far as environmental sustainability is concerned, Morgera [26] argued that international legally binding standards can do more to enforce the responsibility of corporations with respect to environmental sustainability by curbing regulatory arbitrage. Despite these researches identifying the integrity benefits of well-developed legal systems, our research indicates that this regional difference remains with these companies with Asia scoring significantly lower on compliance compared to EU companies. This resembles the findings of Stec et al.[27] discovered that there are in fact no internationally binding norms and that the results of accountability are largely dependent upon the jurisdiction. This heterogeneity also has psychological consequences: individuals in low-enforcement environments have a lower likelihood of feeling that surveillance is legitimate, and it follows that they will less readily volunteer to comply with the surveillance[8, 14]

The frame of reference constructed by Alraziet al.[28] in order to emphasize that the legitimacy of a corporation can be gained using not only a compliance-based approach but also a volunteered approach in addition to a proactive component. This is not an insignificant development, but what is coming under scrutiny is how communities are thinking about the issue of transparency and accountability. Psychological perspective on the impression of standardized ESG The impression of standardizing ESG can produce trust and reduce suspicion, and increase the credibility of environmental monitoring in people's minds [25, 28, 29]. Standardisation of ESG reporting has a connection to better financial performances and more sustainable reported and verified downstream performance, but it is also clear that these voluntary initiatives will not be effective in isolation. Bharti and Kumari[30] echoed other disadvantages of voluntary ESG measures to greenwash business and industry. It serves as a reminder that the standards of a corporate responsibility concept are not a rule of law but indeed a mechanism of contouring fairness or at least how, to humans, they can initiate biometric intervention [31, 32]. This research is in line with the obligatory rather than voluntary measures taken on stakeholders in respect [31].

Corporate control systems and internal control systems should also be compared. These forms of government are open and establish the trust and popular approval upon which environmental surveillance technologies rely [32-34]. According to some other researchers such as Kolk[35], Aluchna et al.[32] and, Schneider et al.[36] governmental intervention, increased transparent disclosure, highly coordinated independent control, could influence the be-followers firms. The researchers in this paper have found that the companies which adhere to the ESG reporting guidelines have low variance concerned profitability and will have the highest score on compliance. However, as Yan et al.[29] remark, enforcement remains a challenging issue to overcome even with better governance. We further analyze and make the assumption that we are to enforce truly in the better governance scenario. The article further adds to this body of literature as it shows how even countries where soft enforcement institutions are in place can dilute the effectiveness of voluntary and compulsory strategies due to the variation in their enforcement mechanisms. Both strong enforcement and involvement in community scored high on a scale of trust in this dichotomy, once again confirming the intuit model in institutional trust and compliance [9, 14]

Just as brilliant this analysis can be, limitations can be present. First, publicly listed ESG reports may not be an ideal source of data, which creates the risk of bias. Companies whose sustainability track records are performing well are advised to publish their data and those companies whose performance is poor may not publish their data. This constraint aligns with the results of Gulluscio et al.[37], according to which selective disclosure distorts the perceived effectiveness of ESG controls. Independent audits or supplementing the self-report data with private survey data to address participant biases could be helpful to longitudinal singing research.

A second disadvantage is that reporting systems vary according to different regions. Standardised systems represent a point of departure but as ESG interpretation is a jurisdictional matter, it is difficult to make a direct comparison. Such discrepancies could be resolved in further new reporting recommendations that were proposed by Schultegger et al.[38] as part of our study, and laws are, of course, being applied differently in various places, and so things that were true in the US or the EU would be different in Asia or Latin America. The asymmetrical pressure on enforcement mitigates somewhat according to et al.[27].

The findings of this study support the appeal of global harsher enforcement requirements and penalties on corporate environmental offenders. Besides showing that the sanctions had to be larger in order to be a deterrent, Bertram [25] and Paduano [39] argued that court rulings would result in increased compliance by establishing a legal precedent. As Bharti and Kumari [30] posit, poor penalty mechanisms do not auger well with corporates in firms that are embracing sustainable practices. Like some researchers support such as Morgera [26] and Stec et al.[27] as a means to increase the application of the rule of law and the adherence to sustainable legislation throughout the world rather than a means to be a platform to maintain the peace established by national law.

The results also show that technologies, such as the AI and blockchain, can be used in order to improve corporate compliance practices. Gadinis and Miazad [40] put emphasis on using next-generation technologies to enhance transparency and eliminate fraud in ESG disclosureIt is this loophole where companies can say they are doing as a way to become sustainable, when they might actually, be breaking a law that must be filled by machine-learning algorithms and AI-approaches, by blockchain validation/root cause claiming systems. We would even desire to go beyond that demanded of a behaviorally apparent, stable, sustainable system and have this integration instilled into processes of participatory communications (rich with informed consent, privacy preservation tools[13, 24], which would foster in turn the call taken by a robust accountability framework and to reinforce the technology to support same.

The interaction between technology and enforcement commitments would then have to be studied further. To clarify; What needs to be done in order to incorporate AI and Blockchain into the existing regulatory framework to achieve a more responsible and transparent environment? How would these technologies help reduce the discrepancies existing between reported and verified ESG data? Along similar lines, longitudinal studies can also take into account the long-term impacts of judicial precedents on corporate conduct, as suggested by Bertram [25] and Sari and Gunadi [41].

Inclusion of larger leaf data and hence expansion of dataset to additional regions and industry areas will also lead to better generalization. Although this study only focused on specific jurisdictions and sectors, future studies should factor in underrepresented areas, including Africa or smaller developing countries. Alrazi et al.[28] and Schuler et al.[34] both of whom recognized the need for multiple data sources to follow global accountability trends. Higher variety of combinations of firm characteristics and regulatory environments may allow researchers to find a larger set of broadly applicable best practices and interventions specific to a region to assist lagging ones.

It does however have giant loopholes, especially in aspects relating to the penalty framework, disproportionate application and voluntary undertakings. Our results contradict the earlier literature and point at success and ongoing problems in the application of transnational corporate accountability. Stakeholders can assist in facilitating a more material positive change in corporate environmental performance by filling these gaps, through better governance and implementation, standard and new technologies harmonization, and so on.

This discussion suggests that we must also address biometric surveillance using psychology (trust, risk perception, norms of compliance, community legitimacy) as well as law and corporate policy. This triangulation underpins the connection between environmental governance work and work concerning social theory as well.

6. Conclusion

The purpose of the article was to think about whether it was possible to design biometric surveillance as a tool of environmental governmental control that is, at least, not fair, but transparent. It does not involve efficiency and technical performance, which can be viewed as the only variables to consider this type of technologies, as shown in the current study. Everyone needs faster response times and even higher capacity to detect, but none of this guarantees that an object will be legitimate in the long term - legitimized. Interpreted public, community and organizational beliefs of legality, fairness and trust play a crucial role in the effectiveness of intervention systems in sensitive fields, including environmental compliance management. And, in a very broad sense, this is where social psychology becomes ethics and law; where any advantages that may accrue can only be realized should the former somehow converge with the latter.

The statistics gathered have been pointing towards an unthinkably unequal world. In general, the degree of compliance, and the desire to comply, is greater in, say, certain sections of the European Union or Canada, where data protection legislation is very stringent and is accompanied by the prospective of a real, teeth-baring penalty. In other places, particularly portions of Africa, Asia and Latin America, there is reduced enforcement, regulation and very little trust. They are also a complicating factor to the issue of voluntary compliance (as they make compliance appear arbitrary), and are a blow to international mutual recognition. To be considered legitimate to the communities under which surveillance technologies are applied, the usage rules need to be transparent and consistently enforced. Should they in fact be socially accepted in the future, it then follows that they should meet not only the legal, but also the psychological needs.

Not least important, the architecture and functionality of the site have provided Biometrics with automatic ethical protection. Though it is more difficult to see this as an overstep and easier to see this as a defensive buy when you are making it very clear that you are applying privacy by design concepts and that you are using secure encryption and that there is accountability surrounding it in the sense of who can access the information. Mistrust, on the other hand, can be transmitted virally when we bump against, or even flirt, with such moral predicaments. Trust could not be coerced, the best thing was that Natural rights were upheld, people told the truth, that trust was won and kept till the security of all was guaranteed. It is most of all a spiritual lesson, and it is a practical lesson: No system, however thoughtful, however clever in its contrivance, will succeed when the hands that put it in place are not entrusted to the hands that must be led through it.

Participation and communication were also found to be important as other findings showed surveillance projects were pre-characterized, when inquiries were solicited, when feedback was sought, when feedback was considered in the process, communities were more tolerant. Such interest, together with the production of a lower resistance, strengthens the perception that such systems are being operated in the common good. In this aspect, the concept of legitimacy is not generated in any legal texts, per se, but through everyday transactions between institutions as well as their subjects. Meanwhile, the study had apparent limitations. The interview and survey data, while rich in detail, were unevenly distributed across regions, and perspectives from Africa, Latin America, and Southeast Asia remain underrepresented. The equations and indices proposed here offer an initial attempt at quantification, but they will require further testing and refinement before they can be considered robust measures. A more diverse dataset and longitudinal research would add considerable strength to future work in this field.

The study shows that biometric surveillance could play a constructive role in addressing environmental crimes, but only under conditions where technological capability is balanced with ethical responsibility and legal coherence, and where public trust is cultivated rather than taken for granted. The path forward will require collaboration across disciplines and borders, with legislators, technologists, ethicists, psychologists, and local communities working together. If such cooperation is achieved, biometric surveillance may evolve not as a symbol of control, but as a transparent and equitable tool for safeguarding our shared environment.

Conflict of interest

The authors declare no conflict of interest

References

1. Kavanagh MM, Baral SD, Milanga M, Sugarman J. Biometrics and public health surveillance in criminalised and key populations: policy, ethics, and human rights considerations. The lancet HIV. 2019.
2. Marciano A. Reframing biometric surveillance: from a means of inspection to a form of control. Ethics and Information Technology. 2018;21:127-36.
3. Evans NWD, Marcel S, Ross A, Teoh A. Biometrics Security and Privacy Protection [From the Guest Editors]. IEEE Signal Process Mag. 2015;32:17-8.
4. North-Samardzic A. Biometric Technology and Ethics: Beyond Security Applications. Journal of Business Ethics. 2019;167:433 - 50.
5. Smith M, Miller S. The ethical application of biometric facial recognition technology. Ai & Society. 2021;37:167 - 75.
6. Neves PC, Afonso O, Silva D, Sochirca E. The link between intellectual property rights, innovation, and growth: A meta-analysis. Economic Modelling. 2021;97:196-209.
7. Bewley-Taylor DR. US concept wars, civil liberties and the technologies of fortification. Crime, Law and Social Change. 2005;43:81-111.
8. O'Neill C, Andrejevic M, Selwyn N, Gu X, Smith G. 'ETHICAL BIOMETRICS' AND THE FACE OF THE CHILD: THE SURVEILLANCE OF CHILDREN WITHIN FACIAL RECOGNITION INDUSTRY DISCOURSE. AoIR Selected Papers of Internet Research. 2021.
9. Hrudey SE, Silva DS, Shelley JJ, Pons W, Isaac-Renton JL, Chik AHS, et al. Ethics Guidance for Environmental Scientists Engaged in Surveillance of Wastewater for SARS-CoV-2. Environmental science & technology. 2021.

10. Gomathy DCK, Geetha DV, Bathrinathan SR, Sripada SK. EXPLORING THE ETHICAL CONSIDERATIONS OF BIOMETRICS IN CYBERSECURITY. INTERANTIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT. 2024.
11. Kisio B, Wa Teresia N. Ethical Implications of Advanced Surveillance Technologies on Law Enforcement: A Case Study of National Police Service in County of Nairobi, Kenya. East African Journal of Information Technology. 2024.
12. Neves JC, Narducci F, Barra S, Proença H. Biometric recognition in surveillance scenarios: a survey. Artificial Intelligence Review. 2016;46:515 - 41.
13. Ng LHX, Lim ACM, Lim AXW, Taeihagh A. Digital Ethics for Biometric Applications in a Smart City. Digital Government: Research and Practice. 2023;4:1 - 6.
14. Fontes C, Perrone C, editors. Ethics of surveillance: harnessing the use of live facial recognition technologies in public spaces for law enforcement2021.
15. Chukreev VA. Personal biometric data as subjects of criminal law protection. Courier of Kutafin Moscow State Law University (MSAL)). 2022.
16. de Groot NF, van Beers BC, Decock L, Meynen G. Accessing medical biobanks to solve crimes: ethical considerations. Journal of Medical Ethics. 2020;47:502 - 9.
17. Kunrong Z, Shuang W, Wenjun X, Yan J, editors. Environmental Monitoring Mobile Law Enforcement System Design2018.
18. Yan WQ, editor Biometrics for Surveillance2016.
19. Collins VJ, editor Mitigate Soft Target's Vulnerability and Prevent Crime Through Biometrics2013.
20. Watney M. Ethical and Legal Aspects Pertaining to law Enforcement use of Drones. International Conference on Cyber Warfare and Security. 2022.
21. Kyriakou K, Apostolaras A, Velentzas P, Syrigos I, Maglavera S, Evangelatos S, et al. Biometrics Data Space: Ensuring Trustworthy and Secure Data Exchange for Suspect Identification. 2024 5th International Conference in Electronic Engineering, Information Technology & Education (EEITE). 2024:1-6.
22. Savastano M, Amendola C, Bellini F, D'Ascenzo F. Contextual Impacts on Industrial Processes Brought by the Digital Transformation of Manufacturing: A Systematic Review. Sustainability. 2019.
23. Savastano M, editor Noncooperative Biometrics: Cross-Jurisdictional Concerns2017.
24. Anderson W, Simske SJ. Forensic Identification of Environmental Sensors Through Challenge-Based Biometrics. IEEE Sensors Journal. 2023;23:15721-31.
25. Bertram D. Judicializing Environmental Governance? The Case of Transnational Corporate Accountability. Global Environmental Politics. 2022;22:117-35.
26. Morgera E, editor Corporate Environmental Accountability in International Law2020.
27. Stec S, Paszkiewicz M, Antypas A. Is the time ripe for global binding norms for corporate accountability. International Journal of Innovation and Sustainable Development. 2017;11:130-48.
28. Alrazi B, Villiers C, Staden CJv. A comprehensive literature review on, and the construction of a framework for, environmental legitimacy, accountability and proactivity. Journal of Cleaner Production. 2015;102:44-57.
29. Yan Y, Cheng Q, Huang ML, Lin Q, Lin W. Government Environmental Regulation and Corporate ESG Performance: Evidence from Natural Resource Accountability Audits in China. International Journal of Environmental Research and Public Health. 2022;20.
30. Bharti P, Kumari P. CORPORATE GOVERNANCE REFORMS: CONTEMPORARY ISSUES OF ENVIRONMENTAL ACCOUNTABILITY. ShodhKosh: Journal of Visual and Performing Arts. 2024.
31. Schilling-Vacaflor A, Lenschow A. Hardening foreign corporate accountability through mandatory due diligence in the European Union? New trends and persisting challenges. Regulation & Governance. 2021.
32. Aluchna M, Roszkowska-Menkes M, Khan SA. Corporate governance perspective on environmental reporting: Literature review and future research agenda. Corporate Social Responsibility and Environmental Management. 2023.
33. Schaltegger S, Etxeberria IÁ, Ortas E. Innovating Corporate Accounting and Reporting for Sustainability – Attributes and Challenges. Sustainable Development. 2017;25(2):113-22.
34. Schuler D, Rasche A, Etzion D, Newton LH. Corporate Sustainability Management and Environmental Ethics. Business Ethics Quarterly. 2017;27:213-37.
35. Kolk A, editor UvA-DARE (Digital Academic Repository) Sustainability , accountability and corporate governance : Exploring multinationals ' reporting practices2017.

36. Schneider T, Leung LR, Wills RCJ. Opinion: Optimizing climate models with process knowledge, resolution, and artificial intelligence. Atmos Chem Phys. 2024;24(12):7041-62.
37. Gulluscio C, Puntillo P, Luciani V, Huisingh D. Climate Change Accounting and Reporting: A Systematic Literature Review. Sustainability. 2020;12:5455.
38. Schaltegger S, Álvarez-Etxeberria I, Ortas E. Innovating Corporate Accounting and Reporting for Sustainability. Sustainable Development. 2017;25.
39. Paduano C. Article: The (Un)Sustainability of UK Company Law: ClientEarth v. Shell Plc. European Company Law. 2024.
40. Gadinis S, Miazad A. Sustainability in Corporate Law. SSRN Electronic Journal. 2020.
41. Agustin Sari NK, Gunadi A. Corporations As Legal Subjects In Environmental Crimes. Journal La Sociale. 2024.