



THE SOCIAL ETHOS AND DIALECTICAL CHARACTERISTICS OF CYBERSECURITY

Buzrukova Nigoraxon To'raxo'jayevna^{1*}

¹Independent researcher of Fergana State University

*ORCID: <https://orcid.org/0009-0001-2601-6049>

<https://doi.org/10.5281/zenodo.23586037>

Abstract: The article interprets cybersecurity not as a collection of technical safeguards but as a social ethos integrating rights, duties, trust and mutual care. It identifies the victim-blaming risk of turning individual caution into absolute responsibility. A multi-level architecture of responsibility is proposed across corporate design, data protection and state guarantees. Responsibility is argued to be proportional to authority, resources, foreseeability and capacity to mitigate harm.

Keywords: cybersecurity ethos, individual caution, corporate accountability, state protection, distributed responsibility, trust, cybersecurity culture.

INTRODUCTION

As digital technologies become an intermediary structure of daily life, education, labor, public services, and interpersonal communication, the issue of the social ethos of cybersecurity is moving beyond the scope of technical security and becoming a philosophical problem that affects a person's presence and self-determination in society. At the heart of the problem is the contradiction between the need to demand caution from the user and the fact that real authority over security infrastructure, design, and control is in the hands of corporations and government institutions. Issues of information security, digital subjectivity, and legal protection are highlighted in local studies [1; 2]. However, equating immunity with concealment of information alone, and security with threat blocking only does not adequately explain how an individual is portrayed, evaluated, and managed in digital systems.

Work in the Russian academic environment provides a conceptual analysis of digital identity, state-citizen relations, technological mediation, and new forms of digital culture [3; 4]. British studies, on the other hand, reveal the structural influence of algorithm, information, and platform power on processes that are seen as simple user choices [5; 6]. Scholars from other countries substantiate the issues of digital governance, autonomy, social ontology, and normative legitimacy in various theoretical positions [7; 8]. These literatures allow us to see technology not as a neutral tool, but as a social institution that distributes rights, opportunity, and recognition.

Three gaps are observed in existing approaches. First, the boundaries of individual prudence and institutional responsibility are often confused. Second, technical accuracy, convenience, or risk mitigation are accepted as a complete measure of moral acceptability. Third, the authority to challenge an individual's own information, profile, or decision is treated as a secondary element. The result is the possibility of attributing security failure to user illiteracy, failing to see the role of corporate design and economic incentives in creating risk. For this reason, it is imperative that socio-philosophical analysis assess the legitimacy of the process, the

ORCID: To'raxo'jayevn: <https://orcid.org/0009-0001-2601-6049>

distribution of damage, and the individual's status as an agency as well as the effectiveness of the outcome.

The aim of the article is to reveal the socio-philosophical essence of the social ethos of cybersecurity and to develop normative evaluation criteria based on the "authority-resource-foresight-harm mitigation" responsibility formula. The research questions are: how does digital mediation reconstruct an individual's state of immunity and security; under what conditions technological opportunity becomes a legitimate social practice; and how should responsibility be shared between the individual, the platform, and the state? Scientific innovation consists in the transfer of cybersecurity responsibility from the "user error" model to a multi-subjective, differentiated system of ethical obligations. The proposed approach is not a set of empirical indicators, but rather a conceptual framework for further legal, institutional, and sociological research.

MATERIALS AND METHODS

The study has a theoretical-conceptual character. The materials were selected from eight targeted scientific sources published after 2016: two from the Uzbek scientific environment, two from Russia, two from Britain, and two from two other countries. The choice of sources is not a representative bibliometric selection; it was structured as a theoretical corpus that allows for a comparison of the social ethos of cybersecurity from local, institutional, axiological, and technological perspectives. Only its conceptual position directly related to the topic was used from each source; empirical conclusions obtained in different contexts are not automatically transferred to the same case.

The methodology combines five methods. Conceptual differentiation distinguishes between categories that appear to be similar but have different normative consequences. Dialectical analysis sees the conflict between the need to demand caution from the user and the fact that real authority over security infrastructure, design, and control is in the hands of corporations and state institutions, as social requirements that condition each other, rather than conflicting interests. Normative reconstruction extracts from the actual technical process the moral conditions necessary for its justification. Institutional analysis determines in whom decision authority, resource, and responsibility are concentrated. The contradictory case method, on the other hand, compares situations in which the same technological tool can be legitimate, and non-legitimate.

A "digital impact episode" has been adopted as a unit of analysis, rather than a separate device or application. In such an episode, information is obtained, an algorithmic or human interpretation is created, a decision is formed that affects the individual's capabilities, and the opportunity to react to that decision arises or disappears. The episode is analyzed in terms of the user's reasonable precautions, the service provider's responsibility to secure design, the organization's responsibility to disclose and compensate the event, as well as the state's legal and infrastructural guarantee, and the digital solidarity of the public. This unit helps to evaluate the technology not only by the result of access, but by its entire social life cycle.

The limitation of the study is that the paper does not provide the result of a new survey, experiment, audit, or statistical measurement. The proposed "authority, resource, foresight-harm reduction" liability formula is a theoretical model and should be empirically tested in the

ORCID: To'raxo'jayevn: <https://orcid.org/0009-0001-2601-6049>

case of different platforms, government information systems, and organizations. Also, because the legal regime of technologies differs across countries and industries, the criteria are not a substitute for a specific normative document. Their task is to break down the problem into transparent questions, make ethical risks visible, and improve the quality of the justification for an institutional decision.

RESULTS

The first result is to define the social ethos of cybersecurity as a normative relationship between an individual and an institution, rather than a separate technical case. In this regard, the individual is not just a source of information or a consumer of services, but a subject who can claim the legitimacy of the classification, interpretation, and decision that applies to him. Local sources indicate the social importance of digital security and subjectivity [1; 2]; and Russian studies illuminate the interplay of identity and the interaction of the digital environment [3; 4]. From this, a normative distinction is made between the "influence" of a technological system on an individual and his or her "judgment" on behalf of the individual.

The first dimension of this distinction is the user's reasonable precautions. Just because a technical system has legitimately obtained the information does not automatically justify its desired subsequent use. The context of the information, its initial purpose, and the scope of the relationship that the individual expects must be maintained. The requirement of the level of authority means that the process has a clear legal and social basis, while the technical and financial resource means that the tool chosen is not redundant over the purpose. Thus, technological opportunity is not equal to moral permission; rather, a stronger opportunity gives rise to a stronger justification obligation.

The second dimension is the service provider's commitment to secure design. Digital systems are not limited to the storage of existing information, but also generate a new conclusion, probability, and profile from it. Such an inference can attribute to it features that the individual does not say, and sometimes does not even know for sure. The British and international literature shows that algorithmic and informed authority is strengthened precisely at this stage of interpretation [5; 6; 7]. Inference from information is therefore treated as a separate normative action, and its purpose, evidentiary quality, and possible error must be disclosed.

The third dimension is the responsibility of the organization to disclose and compensate for the incident. When an individual is not given the opportunity to object, technological classification can become a social fact, unilaterally defining the possibilities of work, service, reputation, or social participation. The potential for harm prevention and the criteria for accountability and reparations keep the agency at this point. The individual's voice is an element that is part of the legitimacy of the decision, not an external complaint to the system. In other words, in the digital environment, subjectivity encompasses not only the power to make choices, but also the authority to discuss and correct the technological interpretation of oneself [8].

The second outcome is the systematization of the structural criteria of the "authority, resource, foresight, harm mitigation" liability formula. The model does not make a two-value judgment of "beneficial or harmful" of a technology; rather, it separately examines its purpose, tool, information flow, decision-making process, and reconsideration. The level of authority and the technical and financial resource represent initial legitimacy, the ability to anticipate risk and

the potential to prevent harm represent the ethical and explanatory quality of the process, and accountability and reparation represent the institutional agency of the individual. The existence of one of the criteria does not automatically compensate for the defect in the others.

The table below translates theoretical analysis into practical audit questions. The "acceptable guarantee" column in the table is not an empirically proven universal standard, but rather a conceptual proposition of this paper. It serves to establish a sequence of questions in the evaluation of a particular platform or system of government, to uncover implicit normative assumptions, and to link the discussion between stakeholders to the evidence.

Table 1. Criteria for Normative Evaluation of the Social Ethos of Cybersecurity

Phase/Scale	Table of Contents	Maqbul kafolat	The main danger
Personality	Password, Authentication, Caution	Reasonable caution	Mutlaq ayblash
Platform	Safe Design and Default Settings	Oldindan himoya	Assign risk to the user
Organization	Storing Information and Incident Response	Instant Message and Coating	Hide
State	Legal, Standard and Critical Infrastructure	Legal guaranty	Excessive control
Community	Alertness and mutual support	Digital Solidarity	Stigmatization

As the table shows, ensuring the social ethos of cybersecurity is not limited to the response after a damage has occurred. A legitimate system combines the ability to anticipate risk, limit the flow of information and decisions, inform the individual, and change the outcome. Otherwise, transparency becomes only the presence of the policy text, consent becomes a one-time mark, and human control becomes an automatic confirmation of the outcome. In this sense, the "authority, resource, anticipation, harm mitigation" accountability formula interprets procedural fairness as its internal architecture, rather than an external appendage of technical design.

The third result is a proportional distribution of responsibility between the individual, the organization, the platform, and the state. Much of the technological process takes place in an infrastructure that the user cannot see; therefore, it is normatively unreasonable to attribute all risk to individual negligence. Whoever determines the purpose of data collection, the design of the algorithm, the retention period, and the practical implication, that entity has a higher responsibility for greater explanation and mitigation of harm. This principle does not deny personal responsibility, but rather defines it within the framework of real authority and resource.

At the institutional level, there is a need to implement a accountability protocol that combines the steps of incident prevention, detection, reporting, victim support, and systematic learning. In such a system, oversight does not end only with a legality check; it also covers the accuracy of the target, the quality of the information, the potential error, the impact on vulnerable groups, the channel of recourse and the outcome of the remediation. A periodic audit should serve to change the behavior of the system, not to produce a document. The results of the audit should be presented in an understandable manner to ethical, legal, and user experience representatives in addition to the internal technical team.

At the individual level, the basic requirement is meaningful agency. Agency is measured not by the sheer number of choices, but by the ability to understand the consequences of the choice, to take an alternative path, and to correct an erroneous decision. Formal consent cannot be a moral basis if the system makes opt-out practically impossible, if withdrawal from the service causes significant social or economic harm, or if the individual is unable to see the profile itself. For this reason, a real guarantee of inviolability and security requires that the claim that "the user has chosen himself" must be verified with specific conditions.

At the collective level, digital security is a problem of trust and solidarity. An individual's information often allows us to draw conclusions about his or her family, colleagues, or network connections as well. Therefore, individual consent does not resolve all ethical issues facing third parties and groups. A full-fledged regime of cybersecurity's social ethos should collectively evaluate individual right, group harm, and the public good, but not use the phrase "common good" to indefinitely squeeze individual agency.

DISCUSSION

The proposed approach sits between two fringe positions in the existing literature. The first position is technological optimism, in which increased security or convenience is seen as sufficient justification. The second position sees any kind of information and automation as an inevitable threat to individual freedom. This paper proposes an assessment of its purpose, design, distribution of powers, and procedural safeguards rather than the technology itself. For this reason, the same technology may be acceptable in a clear, proportionate, and revision situation, and unacceptable in a covert and one-sided situation.

Dialectical analysis insists that security and freedom should not be seen as a zero-sum relationship. A transparent, minimized, and objectionable system increases individual trust and makes security itself more sustainable. Conversely, while excessive surveillance, inexplicable profiling, or automatic denial increases short-term control, it can weaken legitimacy, collaboration, and the quality of information in the long run. Human dignity, then, is not an external constraint on security; it is a source of trust for a secure institution.

At the same time, the "authority, resource, foreseeability-harm mitigation" liability formula does not solve all problems with a single formula. Different areas differ in the severity of the damage, the time constraint, and the alternative means. A quick decision in an emergency may be necessary, but it does not absolve the obligation to further notification, independent review, and compensation. In a low-risk recommendation system, however, user settings and insightful explanation may be sufficient, rather than strict control. The criteria make these contextual differences visible, but do not automatically make the decision.

In the context of Uzbekistan, this approach can be applied in the study of digital public services, educational platforms, financial technologies, biometric identity and social networks. However, the article does not provide an empirical conclusion about specific systems in the country. In the future, the real performance of the criteria will be investigated by combining data from document analysis, user interview, algorithmic audit and complaint practice. Particularly vulnerable groups, digital literacy gaps and denial of service costs should be measured separately.

In practical terms, the first recommendation is to introduce a "normative passport" for each high-impact digital system. It specifies the purpose, the information used, the type of conclusion, the effect of the decision, the impact on vulnerable groups, the person responsible, the channel of appeal, and the deletion period. The passport does not duplicate a technical document; it expresses the social justification of the system in a concise and understandable form. Such a tool creates a common language between public discussion, management decision, and independent audit.

The second recommendation is to measure "human control" not by the existence of a formal operator, but by the authority to substantially modify the decision. When an operator blindly follows an algorithm's recommendation, a lack of time or information prevents the reason from verifying it, the human being in the process does not provide legal and ethical protections. For meaningful control, there must be the authority to see an alternative argument, correct the erroneous information, overturn the decision, and document the reason. The same criterion ties the individual's objection to the actual outcome.

The third recommendation is to assess the harm profile not only by the number of security incidents, but also by the reversibility, duration, audience, and significance of the impact in an individual's life. One-time information leakage, irreversible biometric loss, long reputative footprint, and automatic exclusion from essential service have different moral weights. For this reason, the risk matrix should include the impact on agency, dignity, social recognition, and equal opportunity, as well as probability and financial harm.

A fourth recommendation is to link knowledge within the organization on the social ethos of cybersecurity with independent community and academic expertise. The internal team is well-versed in the system architecture, but may not see a normative flaw caused by conflicts of interest or habituation to normal practice. An external expert, on the other hand, may not have sufficient knowledge of the context. A joint audit coordinates technical evidence, user experience, and ethical justification. The result should be an action plan with a deadline and re-examination, not just a list of recommendations.

CONCLUSION

The study interpreted the social ethos of cybersecurity not as an outward consequence of digital technology, but as a socio-philosophical relationship between an individual, platform, organization, and state that redistributes authority and responsibility. First, it was shown that the existence of a technical capability does not in itself imply its moral acceptability, that every data collection, classification, and decision episode should be justified by purpose, necessity, and proportionality. Second, it was justified that an individual's agency encompasses the powers to view information and interpretation, correct an error, choose an alternative, and challenge a decision, rather than being limited to accepting formal consent or terms of use. Third, the "authority, resource, foresight, harm reduction" liability formula was developed as a conceptual tool that allows a technological process to be evaluated not by the outcome, but by the entire life cycle. Fourth, it was established that responsibility should be distributed in proportion to real authority, resource, foresight, and harm reduction potential, rather than being unilaterally imposed on individual negligence. Fifth, institutional legitimacy should be measured not by transparent policy text, but by the performance of insightful notification, information

ORCID: To'raxo'jayevn: <https://orcid.org/0009-0001-2601-6049>

minimization, meaningful human control, correction, appeal, and independent audit. Sixth, it was argued that security, inviolability, and human dignity are not mutually competing values, but rather complementary conditions for a stable digital institution that maintains individual trust and collective collaboration. The proposed criteria are theoretical constructs that have not been empirically validated; they should be verified using document analysis, interviews, user experience, and algorithmic auditing in the case of digital public services, platform moderation, biometric systems, education, and financial services. Thus, the main conclusion of the paper is that ensuring personal security and integrity is a broader task than increasing the level of technological protection, and requires a procedural justice architecture that allows for the justification, limitation, and revision of digital authority.

The article is limited to theoretical-conceptual analysis; the matrix and criteria in it are not an empirically validated index or ranking. In their application, the nature of the field, the legal regime, the technical architecture, the groups that may be affected, and the existing complaint practices should be taken into account. In further research, the criteria should be validated through expert evaluation, user interviews, real-world decision audits, and comparative institutional analysis.

References / Foydalanilgan adabiyotlar / Литература

1. Azizova M. Political participation and democracy: theory and analysis. 2023. J. 1. No. 1. (p. 68–75). DOI: 10.71337/inlibrary.uz.uzbekistan-science-education.25090.
2. Khalilov A., Qorjovova E. Youth and management: New ideas and youth roles in the political system of Uzbekistan. 2025. (p. 104–112). DOI: 10.71337/inlibrary.uz.mead.116024.
3. Nikiforov A.A. Ontological and political dimensions of risk-reflection: risk society and digital transformation. 2022. T. 18. № 4. (p. 489–503).
4. DOI: 10.21638/spbu23.2022.409.
5. Sokolov A.V., Barsky Y.V. Internet activism as a phenomenon of digitalization of civil activity. 2021. T. 29. № 6. (p. 42–47). DOI: 10.31171/vlast.v29i6.8676.
6. Coleman S. The Is and the Ought of Democracy // European Journal of Communication. 2023. Vol. 38(2). (p. 195–199). DOI: 10.1177/02673231231163750.
7. Bright J., Hale S., Ganesh B., Bulovsky A., Margetts H., Howard P. Does Campaigning on Social Media Make a Difference? // Communication Research. 2020. Vol. 47(7). (p. 988–1009). DOI: 10.1177/0093650219872394.
8. Zuboff S. Surveillance Capitalism and the Challenge of Collective Action // New Labor Forum. 2019. Vol. 28(1). (p. 10–29). DOI: 10.1177/1095796018819461.
9. Kreiss D., McGregor S.C. Technology Firms Shape Political Communication // Political Communication. 2018. Vol. 35(2). (p. 155–177).
10. DOI: 10.1080/10584609.2017.1364814.

