Towards a Victimology of Consciousness

By Professor Viacheslav Tuliakov, National University "Odesa Law Academy"

The rapid development of digital technologies and the intensification of hybrid warfare have transformed communication into a critical arena for both societal interaction and criminal activity. In this context, ensuring the security of communication and protecting the consciousness of individuals from manipulative influences have become pivotal challenges for modern criminology and criminal law (Tuliakov, Savinova, 2024). The emergence of the victimology of consciousness reflects a shift from traditional victimology—focused on physical, property, or social vulnerabilities—towards addressing threats to mental autonomy and free will. Drawing on the concept of "inclusive victim consciousness" as articulated by Vollhardt (2015), which emphasizes perceived similarities across victim groups to foster solidarity and positive intergroup outcomes, this article integrates these insights with the works of Ukrainian legal scholars Natalia Savinova, Yulia Kolomiyets, and Pavlo Fris on criminal law, policy and ideology, as well as the EU acquis and the European Convention on Human Rights (ECHR). It explores the criminological and legal dimensions of securing consciousness, proposes reforms de lege ferenda, and introduces the concept of legitimizing state authority through a victim-centered approach to cognitive security.

In the modern world, where communication serves not only as a means of exchanging information but also as an arena for criminal activities, ensuring secure communication is of critical importance in the criminological domain.

This encompasses preventing the criminal misuse of information channels, from traditional means to digital platforms, particularly in an era of hybrid warfare and widespread digitalization, where communication becomes a target for manipulation. Current threats include cybercrime, such as data interception, account hacking, or interference with protected systems, as well as cybersocial deviance in the form of cyberbullying, stalking, doxxing, or sextortion, and informational attacks, such as mass disinformation, deepfakes, and cognitive manipulation.

Alongside this, the concept of consciousness security emerges, which criminology interprets as the protection of an individual's mental autonomy from manipulative practices, including mass propaganda, destructive rhetoric in wartime, manipulations through social media algorithms that sustain "information bubbles," and the use of psychological triggers for radicalization and recruitment into terrorist or extremist groups.

This forms a new dimension of victimology of consciousness, where traditional victimology, focused on physical, property, or social vulnerability, gives way to threats to mental autonomy and free will, positioning the victim not merely as the owner of stolen data but as a bearer of psychological integrity who loses the capacity for independent choice. Vollhardt's (2015) framework of inclusive victim consciousness highlights how perceiving similarities in victimization across groups can promote solidarity and advocacy, contrasting with exclusive victim consciousness, which emphasizes the uniqueness of a group's suffering and may exacerbate conflict (Vollhardt, 2015). Criminological analysis indicates that mass informational attacks, the spread of disinformation, psychological operations (PSYOPS), and radicalization practices create persistent victimogenic fields, where harm lies in the distortion of cognitive processes and the undermining of trust in one's own perception, transforming

communication from a neutral medium into a tool of criminal influence—from cyberbullying to operations involving artificial intelligence, algorithmic manipulations, and deepfake content (Savinova, 2020).

In the realm of modern criminal law, the legal systems of the EU and Ukraine only partially address these phenomena. The EU acquis in cybersecurity and information services includes Directive 2013/40/EU on attacks against information systems, the NIS2 Directive 2022/2555 on network and information security, and the Digital Services Act (2022/2065) and Digital Markets Act (2022/1925) Regulations, which address content moderation and algorithm transparency, creating frameworks for communication security but only marginally touching on the protection of mental autonomy (European Union, 2013, 2022a, 2022b).

In Ukraine, criminal law regulates these issues through Articles 361–363 of the Criminal Code (cybercrimes), Article 182 (violation of communication privacy), Articles 300–302 (circulation of prohibited literature, pornography, and pimping), and new draft laws on countering disinformation, which are under discussion with consideration of freedom of expression limits (Criminal Code of Ukraine, 2001). Crimes of an ideological nature, aimed at promoting prohibited ideologies, include the production and dissemination of communist and Nazi symbols and the propaganda of communist and National Socialist (Nazi) totalitarian regimes (Article 436-1 of the Criminal Code). This norm, introduced in 2015 as part of decommunization and defascization efforts, with amendments in 2022–2023, establishes liability for public denial or justification of fascist crimes, promotion of neo-Nazi ideology, and the production or dissemination of materials justifying the crimes of totalitarian regimes, with penalties ranging from up to five years of restriction of liberty to up to ten years of imprisonment for aggravated offenses (Law of Ukraine No. 317-VIII, 2015). However, gaps remain evident: the lack of definition and criminalization of crimes against mental autonomy (cognitive security), liability for manipulative use of AI for disinformation or cognitive traps, and protection against mass PSYOPS in armed conflicts, where informational aggression is part of hostilities (Savinova, 2013).

Proposals de lege ferenda include introducing new categories of crimes, such as criminalizing offenses against consciousness security through the systematic dissemination of manipulative materials that affect mental autonomy, analogous to hate speech or terrorism propaganda in the EU, as well as liability for algorithmic manipulations and AI-driven attacks, including deepfakes or neural network influences on an individual's will.

Strengthening guarantees for secure communication requires expanding norms on communication privacy to cover all digital channels with end-to-end encryption and implementing GDPR and Digital Services Act standards into criminal law to criminalize breaches of user confidentiality and data manipulations. Institutionally, this entails establishing cognitive security units within cyberpolice to detect digital manipulations and adopting a victim-centered approach with psychological support for victims, similar to those affected by cyberbullying. All reforms must balance human rights, complying with Article 10 of the European Convention on Human Rights and the case law of the ECtHR (Handyside v. The United Kingdom, 1976; Delfi AS v. Estonia, 2015; Magyar Helsinki Bizottság v. Hungary, 2016), limiting criminalization to harmful manipulations that deprive autonomy without restricting freedom of speech (Council of Europe, 1950).

The concept of legitimizing state authority through the victimology of security adds a new dimension to this analysis, integrating insights from inclusive victim consciousness.

The victimology of security, as part of the victimology of consciousness, views the protection of mental autonomy not only as an individual right but also as an element of legitimizing state authority.

By safeguarding against cognitive threats, the state strengthens its legitimacy, demonstrating its ability to protect fundamental values - free will, psychological integrity, and human dignity. The propaganda of totalitarian ideologies, as defined in Article 436-1 of the Criminal Code of Ukraine, undermines these values, creating ideological threats that necessitate criminal law responses.

According to Kolomiyets (2019), crimes against ideology, including the promotion of communist or Nazi regimes, are encroachments on the ideological foundations of the state, justifying their criminalization to protect societal order and national security (Kolomiyets, 2019). Fris (2005) further emphasizes that criminal law must evolve to address modern ideological threats while preserving democratic principles (Fris, 2005).

Inclusive victim consciousness, as described by Vollhardt (2015, 2021), can foster solidarity among victimized groups, potentially reducing intergroup hostility and supporting reconciliation efforts, which aligns with the victim-centered approach proposed here (Vollhardt, 2015; Vollhardt et al., 2021). However, selective inclusive victimhood, where only certain victim groups are acknowledged based on shared conflict positions, may reinforce hostility and undermine reconciliation, as noted by Maxwell et al. (2024) in their analysis of victimization discourses on social media (Maxwell et al., 2024). Legitimizing authority through the victimology of security involves creating legal mechanisms that not only punish violations but also preemptively protect citizens from manipulative influences, reinforcing trust in state institutions. This is particularly relevant in hybrid conflicts, where informational aggression targets the legitimacy of authority through cognitive manipulations.

In conclusion, modern criminology and criminal law recognize the transformation of criminality in the digital era and hybrid conflicts, where communication and consciousness become new arenas of criminal activity, and the victimology of consciousness opens a new paradigm where individuals are cognitively vulnerable.

As Ukraine integrates into the EU legal space, it must develop mechanisms for expanded criminalization of crimes against cognitive security, including ideological encroachments as outlined in Article 436-1 of the Criminal Code, ensuring secure communication, protecting mental autonomy and free will, supporting a victim-centered approach, and adhering to European standards of proportionality.

Preserving the freedom of consciousness as an element of human dignity and legitimizing authority through protection against cognitive threats, while fostering inclusive victim consciousness to promote solidarity, become key tasks addressing the challenges of the digital era and hybrid warfare.

References

1. Tuliakov V., Savinova N. (2024) Colonizing criminal law: towards new architecture of criminal code *Visnyk Asotsiatsii kryminalnoho prava Ukrainy*, *2*(22), 53-74. Режим доступу: https://doi.org/10.21564/2311-9640.2024.22.313732

2. Savinova, N. (2020). Nasylstvo nad osobystistiu – kryminalni pravoporushennia proty hidnosti liudyny [Violence against the individual – criminal offenses against human dignity]. *Visnyk Asotsiatsii kryminalnoho prava Ukrainy*, *2*(3), 122-138 https://doi.org/10.21564/2311-9640.2021.16.244431
3. Savinova, N. O. (2013). Kryminalno-pravova polityka ta ubezpechennia informatsiinoho suspilstva v Ukraini : monohrafiia [*Criminal law policy and ensuring the information society in Ukraine: Monograph*. Kyiv: Editorial board of the journal "Pravo Ukrainy"; Kharkiv: Pravo.]. Kh. : Pravo, 2013. 292 s.
4. Kolomiyets, Y. Y. (2019). *Kryminalno-pravova ideolohiia: Filosofsko-pravove doslidzhennia* [Criminal law ideology: Philosophical and legal study]. Artsyz: FOP Petrov O.S.
5. Fris, P. L. (2005). *Kryminalno-pravova polityka Ukrainskoi derzhavy: Teoretychni, istorychni ta pravovi problemy*[Criminal-legal policy of the Ukrainian state: Theoretical, historical, and legal problems]. Lviv: Lviv State University of Internal Affairs.
6. European Convention on Human Rights (1950). Article 10: Freedom of Expression. Strasbourg: Council of Europe.
7. European Court of Human Rights. (1976). *Handyside v. The United Kingdom*, Application No. 5493/72.
8. European Court of Human Rights. (2015). *Delfi AS v. Estonia*, Application No. 64569/09.
9. European Court of Human Rights. (2016). *Magyar Helsinki Bizottság v. Hungary*, Application No. 18030/11.
10. Directive 2013/40/EU of the European Parliament and of the Council on attacks against information systems. *Official Journal of the European Union, L 218/8*.
11. Directive (EU) 2022/2555 (NIS2 Directive) on measures for a high common level of cybersecurity across the Union. *Official Journal of the European Union, L 333/80*.
12. Regulation (EU) 2022/2065 (Digital Services Act). *Official Journal of the European Union, L 277/1*.
13. Regulation (EU) 2022/1925 (Digital Markets Act). *Official Journal of the European Union, L 265/1*.
14. Criminal Code of Ukraine (2001, as amended). Articles 361–363, 182, 300–302, 436-1. Kyiv: Verkhovna Rada of Ukraine.
15. Law of Ukraine No. 317-VIII (2015). On the Condemnation of Communist and National Socialist (Nazi) Totalitarian Regimes in Ukraine and Prohibition of Propaganda of Their Symbols.
16. Vollhardt, J. R. (2015). Inclusive victim consciousness in advocacy, social movements, and intergroup relations: Promises and pitfalls. *Social Issues and Policy Review*, *9*(1), 89–120. https://doi.org/10.1111/sipr.12011
17. Vollhardt, J. R., Szabó, Z. P., McNeill, A., Hadjiandreou, E., & Winiewski, M. (2021). Beyond comparisons: The complexity and context-dependency of collective victim beliefs. *European Journal of Social Psychology*, *51*(7), 1138–1157. https://doi.org/10.1002/ejsp.2802
18. Maxwell, C., Selvanathan, H. P., Hames, S., Crimston, C. R., & Jetten, J. (2024). A mixed-methods approach to understand victimization discourses by opposing feminist sub-groups on social media. *British Journal of Social Psychology*, *64*(1). https://doi.org/10.1111/bjso.12785
19. European Union Agency for Cybersecurity (ENISA). (2023). *Threat Landscape 2023: Emerging Trends in Cognitive and Information Security*. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

Disclaimer. This text was translated and edited with the assistance of AI Grok 5. All parts of this message created with the involvement of the mentioned AI technologies have been personally reviewed and edited.