

PERSONAL DATA CRIMES IN THE DIGITAL ENVIRONMENT: A CRIMINOLOGICAL AND THEORETICAL PERSPECTIVE

Sultanova Mashhura Shavkat qizi

*“Central Asian University of Environmental and Climate Change Studies” teacher,
Master of Law*

Sultanovamashhura10@gmail.com

Abstract

The rapid development of information and communication technologies has significantly increased the importance of personal data in modern society. Personal data are widely used in financial, medical, administrative, commercial and social activities, while their unlawful collection, storage, dissemination and use create new opportunities for criminal activity. In this context, traditional criminological approaches require reconsideration because crimes involving personal data are frequently committed in a digital environment characterized by anonymity, speed, borderlessness and transnationality. This article examines the criminological characteristics of personal data crimes from a theoretical perspective, focusing primarily on Rational Choice Theory and Digital Space Theory. The article also considers empirical data concerning criminal cases under Article 141² of the Criminal Code of the Republic of Uzbekistan for the period from 2020 to the first half of 2025. The analysis demonstrates that the digital environment changes both the opportunities available to offenders and the traditional mechanisms of criminal prevention. Particular attention is therefore required to situational factors, perceived risks, accessibility of data and technological characteristics of the digital environment.

Keywords: personal data, cybercrime, criminology, Rational Choice Theory, Digital Space Theory, digital environment, criminal prevention, Uzbekistan.

Introduction

Digitalization has transformed the role of information in contemporary society. Personal data such as a person's name, address, financial information, health

information, identification information and biometric characteristics are increasingly processed through digital technologies. The expansion of electronic services, online banking, digital identification and other technological systems has made personal data an important resource for individuals, businesses and public institutions. At the same time, the growing value and accessibility of personal data have created additional opportunities for unlawful collection, disclosure, dissemination and use.

From a criminological perspective, personal data crimes require particular attention because their characteristics differ from many traditional forms of crime. In a physical environment, the offender and victim may be separated by a relatively limited geographical space, while digital technologies allow criminal conduct to be initiated, executed and continued across different locations. The offender may remain physically distant from the victim, use anonymous or pseudonymous accounts, transfer information rapidly and operate across national borders. Consequently, conventional assumptions concerning the relationship between offender, victim and place of crime become more complicated in the digital environment.

The development of information technologies has therefore created not only new objects of criminal encroachment but also new opportunities and conditions for criminal behaviour. Personal data may be obtained for direct financial benefit, used to facilitate other offences, sold to third parties or disseminated without the individual's consent. The dissertation research underlying this article identifies the growing criminological importance of such conduct and emphasizes the need to study personal data crimes not only from a criminal-law perspective but also through criminological theories.

The purpose of this article is to examine the criminological nature of personal data crimes through two theoretical approaches: Rational Choice Theory and Digital Space Theory. The article also applies these theoretical approaches to empirical information concerning criminal cases under Article 141² of the Criminal Code of the Republic of Uzbekistan.

Theoretical Foundations of Personal Data Crimes

One of the theoretical approaches that can be applied to personal data crimes is Rational Choice Theory. In criminology, this approach is associated particularly with the work of Derek Cornish and Ronald Clarke. The theory considers criminal

behaviour partly through the decisions made by offenders in particular situations. Rather than viewing criminal conduct exclusively as the result of stable personal characteristics, Rational Choice Theory emphasizes the circumstances in which an individual decides whether to commit a particular offence.

The application of this theory to personal data crimes is especially relevant because the digital environment may change the offender's perception of both potential benefits and potential risks. Personal data may have considerable economic or practical value. Information concerning bank accounts, identification documents, telephone numbers, biometric information or other personal details can potentially be used for financial gain or to facilitate further unlawful activities. As a result, the perceived benefit of obtaining personal data may become an important factor in the offender's decision-making process.

At the same time, the offender may perceive the probability of detection as relatively low. Digital technologies can provide opportunities to conceal identity, use false accounts, communicate through encrypted channels and operate from locations physically distant from victims. Therefore, where the expected benefit is perceived as significant while the probability of identification or punishment is perceived as limited, the digital environment may create favourable conditions for criminal decision-making.

This does not mean that every personal data crime is the result of a completely rational calculation. Human decision-making can be affected by emotions, limited information, social circumstances and technological circumstances. Nevertheless, Rational Choice Theory is useful because it draws attention to **situational factors** that may make personal data crimes more attractive or easier to commit.

For example, the accessibility of a database may affect an offender's decision. If personal data are poorly protected, easily accessible or available through unauthorized channels, the practical effort required to obtain them may be reduced. Similarly, if an offender believes that the victim is unlikely to discover the violation or that law-enforcement authorities will face difficulties identifying the perpetrator, the perceived cost of the offence may decrease.

Thus, from the perspective of Rational Choice Theory, prevention should not focus exclusively on the offender. It should also reduce criminal opportunities. Increasing the security of databases, limiting unauthorized access, improving monitoring

mechanisms and increasing the likelihood of detection can influence the situational conditions surrounding the offence.

Digital Space Theory

A second important theoretical perspective is Digital Space Theory. Traditional criminology has historically paid significant attention to physical environments such as cities, neighbourhoods, workplaces and other geographical locations. However, personal data crimes frequently occur in a digital environment where geographical boundaries have a fundamentally different meaning.

The digital environment is characterized by several features that are particularly significant for criminological analysis: borderlessness, anonymity, speed and transnationality. These characteristics are identified in the dissertation as important elements distinguishing crimes committed in cyberspace from conventional forms of criminal behaviour.

First, borderlessness means that digital information can move between jurisdictions without the physical movement normally associated with traditional crime. A personal-data violation may involve a victim in one country, an offender in another country and a digital platform or server located elsewhere. This creates practical difficulties in investigation, evidence collection and international cooperation.

Second, anonymity may reduce the visibility of the offender. Although complete anonymity is not always possible, digital technologies can make the initial identification of an offender more difficult. The use of pseudonyms, multiple accounts and other concealment techniques can create additional investigative challenges.

Third, speed distinguishes digital crimes from many traditional offences. Personal information can be copied, transferred or disseminated almost instantaneously. Once information is unlawfully obtained, it can potentially be distributed to numerous recipients within a very short period of time. Consequently, the harm associated with the disclosure of personal data may continue even after the original act has ended.

Fourth, the transnational nature of digital activity creates jurisdictional problems. A criminal act involving personal data may have effects in several states simultaneously. This means that effective prevention and investigation may require

cooperation between law-enforcement institutions, private companies and data-protection authorities from different jurisdictions.

Digital Space Theory therefore expands the criminological understanding of personal data crimes. The central question is no longer only *who committed the crime and against whom*, but also *how the characteristics of the digital environment created the opportunity for the offence*.

Interaction Between the Two Theories

Rational Choice Theory and Digital Space Theory can be considered complementary in the analysis of personal data crimes. The first focuses primarily on the offender's decision-making and the perceived benefits and risks associated with criminal behaviour. The second focuses on the environment in which that decision takes place.

For example, an offender may perceive personal data as economically valuable. At the same time, the digital environment may provide relatively easy access to such information and create physical distance from the victim. The combination of economic motivation and favourable technological circumstances may increase the opportunity for criminal conduct.

Therefore, personal data crimes can be understood as the result of an interaction between individual decision-making and environmental opportunities. This approach is particularly relevant for prevention because it suggests that reducing crime requires both individual-level and situational measures.

Criminological Characteristics of Personal Data Crimes in Uzbekistan

The theoretical analysis can be supplemented by empirical information concerning criminal cases under Article 141² of the Criminal Code of the Republic of Uzbekistan. The dissertation examined completed criminal cases for the period from 2020 to the first half of 2025. The analysis provides several characteristics of persons convicted of this category of offences.

According to the study, there was a significant gender difference among convicted persons. Approximately 90% were men, while 10% were women. This empirical finding describes the composition of the cases examined in the research and should not, by itself, be interpreted as demonstrating that gender is a direct cause of personal data crime. Rather, it indicates a distributional characteristic within the studied criminal cases.

The age distribution is also notable. Persons aged 26–35 accounted for 55% of the studied cases, while those aged 36–45 represented 22%. Persons aged 18–25 accounted for 19%, and the group aged 46–60 represented 4%. Thus, the largest proportion in the examined material belonged to the 26–35 age group.

These findings can be considered alongside the theoretical framework. Individuals who are active in employment, financial transactions and digital services may encounter a broad range of personal-data systems and technological opportunities. However, the available empirical data do not establish a direct causal relationship between age, employment activity and criminal behaviour. Further research would therefore be necessary to determine the specific social, economic and technological factors underlying the observed distribution.

The criminological analysis also demonstrates the importance of examining the relationship between personal data crimes and other forms of criminal activity. Personal data may not always represent the final objective of the offender. Unlawfully obtained information can create opportunities for subsequent financial, fraudulent or other criminal conduct. Consequently, the protection of personal data can have a preventive function beyond protecting privacy alone.

Key Challenges in the Prevention of Personal Data Crimes

The digital environment creates several challenges for the prevention of personal data crimes.

The first challenge is the rapid development of technology. Criminal legislation and institutional mechanisms may develop more slowly than technological practices. New technologies can create forms of data processing and dissemination that were not contemplated when existing criminal-law provisions were formulated. The dissertation specifically identifies concerns regarding the ability of the existing legal framework to fully address technologically sophisticated conduct, including the mass sale of personal databases through the Darknet and unauthorized processing of biometric information through artificial intelligence.

The second challenge is difficulty in identifying offenders. Anonymity and the use of digital technologies can complicate the collection of evidence and identification of persons responsible for unlawful acts.

The third challenge is the transnational character of digital crimes. Where different elements of an offence are located in different jurisdictions, investigation may

require international cooperation and access to evidence held by foreign institutions or private technology companies.

The fourth challenge concerns the speed of dissemination. Traditional preventive mechanisms may be insufficient when personal information can be copied and distributed almost immediately. Prevention therefore requires not only punishment after an offence has occurred but also technical and organizational mechanisms capable of reducing opportunities for unauthorized access.

In this context, the dissertation proposes strengthening the criminal-law response to technologically facilitated violations of personal-data protection. One of the proposed approaches is to introduce the use of information and communication technologies, including the Internet and artificial intelligence technologies, as an aggravating qualifying circumstance within Article 141². The dissertation also proposes a separate Plenum decision of the Supreme Court concerning judicial practice in cases involving cybercrime and violations of personal-data privacy.

Conclusion

Personal data crimes represent a distinctive area of contemporary criminology because they develop at the intersection of criminal behaviour and digital technology. The digital environment changes the traditional relationship between offender, victim and place of crime and creates new opportunities for unlawful access, use and dissemination of personal information.

Rational Choice Theory provides a useful framework for examining the situational factors influencing criminal decision-making, particularly the perceived benefits, risks, accessibility of information and probability of detection. Digital Space Theory complements this approach by emphasizing the characteristics of the environment in which these crimes occur, including anonymity, speed, borderlessness and transnationality.

The empirical analysis of criminal cases under Article 141² of the Criminal Code of Uzbekistan for 2020–the first half of 2025 demonstrates identifiable characteristics within the studied cases, including the predominance of male convicted persons and the concentration of cases among the 26–35 age group.

The combination of theoretical and empirical analysis suggests that the prevention of personal data crimes should not rely exclusively on post-criminal punishment. It should also address the technological and situational conditions that create criminal

opportunities. Strengthening digital security, improving institutional monitoring, increasing the effectiveness of detection mechanisms and developing criminal-law responses to technologically facilitated violations are important components of an effective preventive strategy.

Ultimately, the criminological study of personal data crimes requires a shift from a purely offender-centred approach toward a broader analysis of the interaction between offender decision-making, technological opportunities and the characteristics of digital space.

References

1. Cornish, D. B., & Clarke, R. V. *The Reasoning Criminal: Rational Choice Perspectives on Offending*. New York: Springer-Verlag, 1986.
2. United Nations. *Universal Declaration of Human Rights*, Article 12.
3. United Nations. *International Covenant on Civil and Political Rights*, Article 17.
4. UN Human Rights Committee. *General Comment No. 16: Article 17 (Right to Privacy)*, 1988.
5. United Nations General Assembly. *The Right to Privacy in the Digital Age*, Resolution 68/167, 2013.
6. United Nations General Assembly. *The Right to Privacy in the Digital Age*, Resolution 69/166, 2014.
7. Republic of Uzbekistan. *Law on Personal Data*, 2019.
8. Criminal Code of the Republic of Uzbekistan, Article 141².