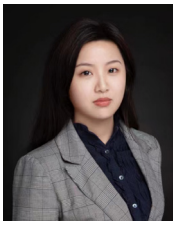
Original paper

УДК 159.99
DOI: 10.35750/2713-0622-2024-4-544-556

Application of legal psychology in risk prevention mechanism of digital society



Zhang Boge
Shanghai Police College
(Shanghai, China)

Abstract

The study of legal psychology can actively promote the legal adjustments of traditional social relationships, which is already reflected in the current legislation in China. Provisions regarding the mental health of citizens can be found in various written laws and legal articles. For example, the Criminal Law clearly distinguishes the criminal responsibility of mentally ill patients, while the Administrative Penalty Law has special provisions regarding the cognitive status of intellectually disabled individuals. In terms of judicial practice, in response to the increase in juvenile delinquency issues in recent years, the Supreme People's Court and the Supreme People's Procuratorate have issued multiple judicial interpretations to provide case guidance. In the rapidly developing era of informatization, facing the emergence of a digital society such as the "metaverse", it is crucial to exploit the future research emphasis of legal psychology.

Keywords

legal psychology, social psychology, sociology

For citation: Zhang Boge (2024). Application of legal psychology in risk prevention mechanism of digital society. *Russian Journal of Deviant Behavior*, 4 (4), 544–556. doi: 10.35750/2713-0622-2024-4-544–556.

Оригинальная статья

Роль юридической психологии в механизме предупреждения рисков, связанных с развитием цифрового общества

Боге Чжан
Шанхайское высшее училище полиции Министерства общественной безопасности Китайской Народной Республики
(Шанхай, Китай)

Аннотация

Развитие юридической психологии способствует корректировке традиционных общественных отношений и находит отражение в законодательстве Китайской Народной Республики. Положения, учитывающие психическое состояние и здоровье граждан, можно найти

в различных нормативных правовых актах и законах. Например, в Уголовном кодексе Китая представлена уголовная ответственность психически больных лиц, а в законе об административных наказаниях есть специальные положения, касающиеся когнитивного статуса умственно отсталых лиц. Что касается судебной практики, то в связи с ростом количества преступлений, совершенных несовершеннолетними, Верховный народный суд и Верховная народная прокуратура разрабатывают методические рекомендации, регулирующие данный аспект работы. В стремительно развивающуюся эпоху информатизации, перед лицом возникновения цифрового общества, крайне важно использовать исследовательские возможности юридической психологии для познания и регулирования цифровой «метавселенной».

Ключевые слова

психология цифрового пространства, юридическая психология, юридическая социология

Для цитирования: Боге Чжан (2024). Роль юридической психологии в механизме предупреждения рисков, связанных с развитием цифрового общества. *Российский девиантологический журнал,* 4 (4), 544–556. doi: 10.35750/2713-0622-2024-4-544–556.

For a long time, psychology has been a discipline in China with high scientific costs and low social effectiveness. Legal psychology, as an interdisciplinary field of law and psychology, applies general psychological principles to study various psychological activities related to legal behavior and their patterns. From a specific application perspective, the main tasks of legal psychology can be roughly summarized as follows: through the exploration and research of the psychological activities of criminal subjects and law enforcement personnel in law enforcement practice, clarify the subjective and objective factors that lead to illegal behavior; seek to educate and reform offenders according to the objective laws of psychological change; reduce or eliminate social psychological factors and individual personality traits that contribute to criminal behavior, thus promoting the establishment of the rule of law and accelerating the process of legal socialization. The first stage of the development of legal psychology was closely linked to criminal law, and its study began with research on criminal psychology. Criminal psychology originated from the research of the Italian psychiatrist Lombroso. In the late 19th century, Russian scholars delved into the analysis of criminal behavior by applying the early results of clinical psychology in the field of law. Most of the focus was on studying juvenile offenders or studying the subjective factors of criminals such as personality and attitudes, gradually forming some legal psychological ideas. During the Soviet era, the formation of legal consciousness and key factors in the study of criminal behavior, such as responsibility, intent, negligence, complicity, and other definitions with a psychological background, all required the development of legal psychology.

The development of new productivity in modern society has brought about a series of new propositions, such as the psychology of legislative activities (the design of new laws, improving the efficiency of existing legislation), the formation of legal culture psychology, citizen litigation psychology, jury trial psychology, criminal re-socialization and rehabilitation psychology, legal extremism psychology serving in local conflict areas, psychology support for fighting terrorism, psychology semantics of legal conflict studies, the formation of social perspectives on the activities of legal agencies and their images, and the issue of professional burnout, etc. Therefore, we must see that legal psychology and criminal psychology should have a general and individual relationship, the former needing to generalize psychological laws concerning legal activities at a higher level to guide research in all branches of knowledge, including criminal psychology.

1. Evolution of Digital Society and Endogenous Risk

Digital society is a social form composed of both virtual and real elements, which is different from traditional society and not the same as cyberspace. In a digital society, the virtual and real societies

intertwine but also have distinctions. The operation of the virtual society relies on electronic devices such as mobile phones and computers, with its institutions, rules, algorithms, and ethics closely linked to the real society, yet different in terms of interaction methods and operational logic. The binary nature of digital society gives it uniqueness, and we can understand its basic structure through a binary analysis framework of virtuality and reality, which includes three typical types: pure virtual society (such as virtual worlds in games and movies), pure real society (everyday activities in the physical society), and digital society combining virtual and real elements (including forms of fusion like augmented reality, immersive experiences, and role-playing).

China's digital society began in the 1990s with the birth of the information Internet, especially after full access to the international Internet in 1994, ushering in the era of digital information. Initially driven by research institutions, the construction of Internet infrastructure laid the foundation for the WEB1.0 society or information society. The digitization of social interaction has become a notable feature of the digital society, with the number of Internet users surpassing 100 million in 2005. The rise of social networking sites marked a shift in the role of Internet users and the expansion of social relationships on digital platforms. With the advent of a social media-driven WEB 2.0 society, the human digitization process has accelerated. In 2019, the commercialization of 5G technology and the outbreak of the new crown epidemic further promoted digital transformation, with rapid development in areas such as the Internet of Things, digital economy, and digital governance. The digitization process of public services and life scenes has been accelerated, creating a new type of digital life characterized by smart sharing. In the future, the concept of the metaverse heralds further development of the digital society, utilizing cutting-edge technology to create a virtual world that interacts with the real world, showcasing the digital living space of a new social system. The metaverse is seen as a new evolution of Internet technology, a new sign of human existence, and an advanced form of digital existence. It represents the virtualization and digitization process of the real society, as well as the emergence of a new social ecology based on the digital environment. The metaverse is not only the embodiment of an intelligent society, but also a super-intelligent society where virtuality and reality intertwine and merge, possibly aligning with "Society 5.0" or other more advanced social models.

From the perspective of material distribution in the digital society, driven by digital technology and artificial intelligence, material production has become more efficient through data optimization, encoding, and integration. At the same time, social wealth is increasingly concentrated in the hands of individuals who have data power. This concentration leads to the exclusion of individuals who fail to control data, resulting in a new type of economic marginalization risk. With the infiltration of capital into digital life, the wisdom and creativity of workers are becoming more standardized, lacking diversity. Compared to the poverty issues directly caused by mechanized production in the industrial era, the digital age's digital displays and games have surpassed traditional functional boundaries, making the concept of poverty increasingly unclear. However, it can be affirmed that those who cannot control data will mostly fall into the trap of becoming "data collectors" or "abandoned individuals", thus falling into a new form of poverty. At the same time, a minority of people who possess a large amount of crucial data have become the "digital elites" dominating society, wielding immense power and influence. In short, the digital society is a complex social form. Its development is changing the way we live and work, providing unprecedented convenience and opportunities, but also bringing new challenges and issues.

2. Major Legal Risks of Digital Society

The development of information technology aims to better satisfy people's yearning for a better life and promote human freedom and liberation to a greater extent. However, digital society is a highly developed digital society, in which everything is monitored, human beings are like "streaking" in front

of cameras, and people's privacy is at risk of being digitized indefinitely. Therefore, it is generally believed that the greatest risk to digital society is the risk of loss of individual privacy. China formally implemented the Law of the People's Republic of China on Personal Information Protection on November 1, 2021, which plays an important role in effectively protecting the rights and interests of personal information. However, in the digital era, the breadth, strength, and validity of personal information protection still face severe challenges.

However, we should also note that in the process of building a digital society, interpersonal relationships, transaction relationships, production patterns and consumption patterns have undergone fundamental changes from the physical world to the digital world. In interpersonal relations, almost everyone in the world can communicate widely through digital media. Digital interpersonal relations are both "sparse" and "far", which has an invisible impact on many social movements and social ideas. In terms of transaction relations, market transaction relations, service transaction relations, product transaction relations, labor transaction relations and currency transaction relations have undergone unprecedented changes due to digitalization. Digital transaction relations are very "convenient", but full of "uncertainty"; In production mode, intelligent production equipment and automation of production process, digital production mode change is both "efficient" and "accurate", but digital production mode accelerates the evolution speed and "de-socialization" degree of human beings; In terms of consumption patterns, digital consumption platforms, digital logistics platforms, digital promotion platforms and digital after-sales platforms have created more imaginative ways and forms for human product consumption and service consumption, but they have also created some kind of "trap" for human beings. Therefore, the digital society era needs to re-examine the methodology and risk concept of the digital world. These over-emphasize the digital characteristics of digital society, while ignoring the social attributes of digital society, which easily makes people feel lonely, thus causing depression, apathy, depression, loss, and other mental health problems. Therefore, in the construction of digital society, we should strengthen the technology and scene design in group interaction and social interaction.

Accompanying this, the digital society may see a large number of robots present, and the interaction between humans and robots will become more frequent. In this interactive process, humans may slowly start to see themselves as robots through their interactions with robots, and even classify some humans as being inferior to robots. Over time, this could lead to some humans alienating themselves to become robotic-like individuals, gradually losing their humanity. Therefore, in the process of governing the digital society, particular attention must be paid to the changes in human nature.

i. The new network-based crime poses a significant threat to minors.

With the accelerated development of social digitalization, the widespread application of information technology has profoundly changed people's ways of life, while also creating new evolving spaces for traditional crimes. Particularly in the realm of sexual offenses, the internet has become a new tool and platform for criminals. The prevalence of the internet and the rise of social media make it easier for sexual offenders to contact potential victims, while the anonymity of the internet and big data technology provide opportunities for concealing and evading sexual crimes. The anonymity provided by networks like the dark web has created a hidden platform for sexual crimes, making it more difficult for law enforcement to combat. The development of artificial intelligence technology has also provided new tools for the application of technologies such as virtual reality and augmented reality in the pornography industry. Traditional sexual crimes such as sexual assault and harassment have now spread to the virtual world, leading to an increase in online sexual crime cases. For example, the dissemination of pornographic materials, cyber harassment, and even sexual assault using deep fake technology are not only difficult to track but also cause immense psychological harm to the victims.

In the face of these new forms of sexual crimes, society and individuals need to strengthen publicity and education, strengthen legal and law enforcement efforts. At the same time, technology companies and internet platforms should also take on the responsibility of supervision and filtering, together dealing with and combating these issues, protecting the safety of society and the rights of individuals.

Recently one intermediate People's Court ruled on a case of child molestation using the internet. The defendant, Mr. Shu, actively befriended multiple underage victims aged 7 to 14 on online platforms with the aim of seeking sexual stimulation in four years. He used the internet to entice, coerce, and manipulate these victims into sending him intimate photos and videos of their naked body parts, bathing, and masturbating for his viewing pleasure. He then proceeded to share and distribute these materials on the internet or with others. Such acts of molestation, when carried out through the internet, often exhibit a level of gravity, duration, number of victims, and harmful consequences that surpass traditional offline acts of molestation. Due to the covert and persistent nature of online sexual harassment, often accompanied by seductive behavior, the perpetrator frequently uses deception, coercion and other means to demand the victim's private photos and videos, leading the victim to be dominated and coerced for a long period of time. This can easily result in severe psychological issues such as low self-esteem, self-disgust, and social withdrawal, causing great harm to the physical and mental health of minors. At the same time, it instills fear in the victim and their guardians of the potential dissemination of private photos and videos, keeping them in a state of perpetual anxiety.

Such criminals use online platforms to disseminate pornographic and obscene information, polluting the social atmosphere and harming the physical and mental health of minors. Some criminals also contact minors online by pretending to be nearby friends, concealing their age and occupation, getting close to minors through online chatting, sending red packets, etc., taking advantage of minors' innocence to entice them to send naked photos or engage in nude chats or even arranging to meet in person to exploit opportunities to harm minors. Recently, there has been a rise in "naked loans" crimes targeting minors and college students, severely infringing on the rights of minors. Therefore, with the digital transformation of society, in terms of social governance methods, we must strengthen cyber security education, improve relevant laws and regulations, enhance network monitoring and crime investigation capabilities, in order to protect the network security and privacy rights of citizens, and prevent sexual crimes from generating new threats in the digital age. In terms of legal education for individual citizens, we should be adept at using the scientific tool of legal psychology, utilize big data analysis to study the behavioral patterns of some digital netizens, predict whether they are potential sexual offenders, and establish an early warning system.

ii. The Societal Hazards of Telecom Network Fraud

Telecom network fraud, as a type of non-contact, intelligent, and highly networked new crime, has become a prevalent and serious form of criminal activity in China. Compared to traditional crimes, telecom network fraud exhibits more intelligence, swiftness, non-contact nature, as well as characteristics of cross-regional and cross-national scope. Since the enactment of the Anti-Telecom Fraud Network Security Law in 2022, China has maintained a strict and high-pressure stance against cybercrime. In 2022, the national procuratorial organs prosecuted a total of 31,000 people involved in telecom and internet fraud crimes. From April 2021 to July 2022, the national public security organs successfully cracked 594,000 cases of telecom and internet fraud. In order to decisively curb the high incidence of telecom and internet fraud crimes, the Ministry of Public Security continues to deploy special operations, organize regional battles and group campaigns, and harshly crack down on criminal gangs involved in providing illegal services such as promoting and directing overseas fraud groups, money laundering through transfers, technical development, and organizing illegal border crossings. 79,000 criminal suspects have been arrested, including 263 masterminds and key figures behind the

scenes of fraud groups. As of January 9, 2024, according to statistics, national public security agencies across the country have successfully cracked down on a total of 437,000 cases of telecommunications network fraud in 2023. With the strong cooperation from all sides in Myanmar, a total of 41,000 suspected criminals involved in telecommunications network fraud were handed over to our side in 2023[1].

Typical online fraud schemes include:

1. Impersonation fraud. Criminals deceive others by impersonating leaders, friends, organizations, etc., for example, pretending to be a leader's secretary or staff to promote books, commemorative coins, etc., or pretending to be friends to ask for help in emergencies, and using instant messaging tools to steal account passwords and then impersonate the account owner for fraud.

2. Shopping fraud. Fraud is carried out through false discount information, customer service refunds, fake online stores, etc., including fake customer purchases, refund fraud, online shopping fraud, low-price shopping fraud, and installment payment fraud release fraud, etc.

3. Incentive fraud. Using tempting winning information, rewards, high salaries, etc. to lure users into fraud.

4. Online gaming and trading platform fraud. Including pretending to be a game friend borrowing money, online game equipment and game currency trading fraud, and using social platforms for fraud.

5. Brushing fraud. Suspects of the crime recruit personnel for online part-time brushing through promoting part-time job advertisements, and then refuse to refund for various reasons and blacklist them.

6. Credit card and loan fraud by proxy. By publishing phishing websites for credit card applications, loans, and other scams, illegal access to citizens' personal information is obtained, followed by impersonating bank employees or loan company staff to contact victims, in order to carry out scams under the guise of paying fees, annual interest rates, deposits, etc.

7. Network dating fraud leading to gambling and investment scams. By posing as single users on marriage and dating websites, trust is built through a period of communication before establishing a relationship with victims, leading them into gambling or investment scams. Taking the scam method known as "kill fish plate" as an example, it involves specific tactics: firstly, false information such as increasing credit card limits, cashing out Huabei, and applying for low-interest loans without collateral are published, attracting victims through pre-designed false links on the internet, and then deceiving victims into transferring money with various reasons such as unfreezing fees or benefits; secondly, using online shopping platforms to publish second-hand goods information to attract victims, and then gaining their trust to trick them into clicking on false links to place orders.

All telecommunications network fraud activities are characterized as group crimes with clear and detailed division of labor among the criminals. In planning the entire criminal operation, meticulous arrangements are made for each stage of the crime, including the existence of training scripts. Through these training scripts, victims are subjected to scenario induction, brainwashing reconstruction, and resistance elimination in order to establish psychological control. The training scripts serve as a tool for fraud groups to control the minds of the victims and elicit desired reactions. They penetrate the patterns of reactions in victims at various stages of psychological control, for example, by providing certain stimuli to the victims to elicit specific responses. Based on the understanding of the correspondence between the stimulus and response of the victim, fraudsters pre-set the plot of the scam, arrange fictional characters, and drive the situation switch to control the reduction or excessive input of scam

[1] *Ministry of Public Security, People's Republic of China. Combat and Control of Telecommunications and Internet Criminal Activities* – Key News Focus [EB/OL] (Accessed April 15, 2024). https://www.mps.gov.cn/n2255079/n4876594/n5104076/n5104077/index.html

information to "brainwash" the victim, "inducing" the victim to actively fall into the scam trap, and eventually make the transfer. As the rhetoric system understands and exploits the "frame-first" in the model of human psychological reactions, the victim unknowingly accepts rhetorical induction and indirect suggestions, completing deceitful transfer "tasks" according to the instructions of the fraudsters.

iii. The dilemma of platform liability for infringement in digital monopolies

With the integration of digital technology into various fields, infringement behaviors have become more concealed, and the decrease in infringement costs has led to the rampant proliferation of piracy and infringement activities. Digital infringement has characteristics such as virtuality, multiplicity of subjects, indirectness, and synchronicity in time and space, making the causal relationship between infringement behavior and its consequences complex, posing a challenge to the application of existing infringement legal norms. The existing legal framework may be difficult to fully adapt to the development speed of digital technology, which requires legislators to analyze the causes of the regulatory dilemma of digital infringement responsibility, study principles of attributing digital infringement, elements of liability, and remedies for damages, and explore the adaptability and lag of existing laws to digital infringement.

In the context of globalization, digital infringement often crosses national borders, which requires different countries and regions to coordinate their legal systems in order to jointly address digital infringement issues. This involves not only the establishment and enforcement of laws, but also international judicial cooperation and legal assistance, as well as the establishment and improvement of regulatory mechanisms for digital content, including copyright registration, monitoring, tracking, and enforcement. This is crucial for preventing and combating digital infringement. In addition to using legal and information technology methods, raising public awareness of digital copyright protection is also key to addressing digital infringement issues. This can be achieved through legal education and publicity to enhance the public awareness of the importance of intellectual property rights, and also fundamentally reduce the possibility of infringement. In the digital environment, the responsible parties may involve multiple participants, such as platform operators, content providers, and technology service providers.

As one of the main actors in digital social governance, digital platforms are built on digital technology, providing a means of communication and interaction. They serve as the infrastructure of digitization, facilitating interactions between two or more groups. These platforms are often capital-led, leading to the centralization and monopolization of data resources. The origins of these platforms are typically linked to addressing internal data needs, gradually evolving into powerful tools for monopolizing and exploiting the growing amounts of data. This control and utilization of data can be likened to the production hegemony described by Jean Baudrillard. He views it as a secondary rule, where machines and robots dominate over living labor, and dead labor exerts control over living labor. In the context of digital platforms, data has become a new form of hegemonic mechanism to control and extract intellectual output from laborers. Traditional working days have evolved into digital working days without clear boundaries, where rest and work time become blurred. Digital platforms constitute a form of super-monopoly, not only plundering the value created by workers during working hours but also exploiting their lifetime, placing every moment of life under the strict control of data systems. The transformation of digital life means that lifetime shifts from a factory-style ownership mechanism to a state dominated by the entire data system.

The unsustainable risks of the digital platform ecosystem and the design of a new anti-monopoly system: As an important driving force for the economic development of our country, digital platforms maintain a high-speed development momentum, and have attracted high attention from

the government. Data from the "Observation of Platform Economy and Competition Policy (2021)" shows that from 2015 to 2020, the market value of digital platforms in China with a market value of over $1 billion increased at a compound growth rate of up to 35.4%. On the one hand, the rapid development of digital platforms has had an impact on the socio-economic sectors; on the other hand, the unique competitive ways of digital platforms also challenge the operational order of traditional markets, prompting the government to pay attention to the standardized development of platforms. Since 2021, various departments have successively issued documents such as "Guidelines on Anti-Monopoly in the Platform Economy Field," "Internet Platform Classification and Grading Guidelines (Draft for Solicitation of Comments)," "Internet Platform Implementation of Subject Responsibilities Guidelines (Draft for Solicitation of Comments)," and "Several Opinions on Promoting the Normative and Healthy Development of the Platform Economy" to gradually improve the governance system of digital platforms. It is important to adhere to the task of promoting the normative, healthy, and sustainable development of the platform economy, which includes clarifying the various risks that may exist in the current digital platform ecosystem and taking corresponding measures to prevent them. Among various risks, the risk of digital platform monopolization is a crucial aspect, and it is of great significance to further develop a targeted and more reasonable anti-monopoly system based on the current anti-monopoly practices.

The monopoly of data not only harms the interests of consumers, but may also lead to various issues such as decreased market efficiency, limited innovation, reduced market competition, data security risks, distortion of economic resource allocation, regulatory challenges, social fairness issues, risks of economic fluctuations, and decreased international competitiveness. Assessing the extent and scope of the losses, as well as effectively seeking damages, is an important issue in determining liability for digital monopolies. Identifying the liable parties and how to allocate responsibility among these parties is another complex issue. This requires consideration of the roles and contributions of all parties, as well as their ability to control and their interests in preventing infringement.

3. Leveraging the analysis of group digital behavior characteristics to strengthen the construction of digital rule of law

Social psychology is the psychological representation of the characteristics of the times, and social mentality is formed under the influence of the social environment and culture of a certain period. The common and consistent psychological characteristics and behavioral patterns exhibited by the majority of members in society become a template that influences the behavior of individual members. Analyzing the causes and influencing factors of digital social crises: Legal psychology can analyze the causes and influencing factors of digital social crises, thus providing a scientific basis for formulating effective countermeasures. Analyzing the psychological characteristics of online fraud can help us develop more effective prevention and enforcement measures. By examining judicial cases and precedents related to digital social crises, legal psychology can extract experiences and lessons to guide future judicial practice. For instance, analyzing legal cases involving violations of personal privacy online can enhance our understanding of privacy protection laws and practical applications. Exploring approaches and mechanisms for resolving digital social crises, legal psychology can provide support for mediating and resolving such crises. Exploring the mediation mechanisms and solutions for online disputes can help the parties involved resolve issues more harmoniously.

i. The application of forensic psychology in the prevention mechanism of cybercrime.

By analyzing a person's character, it is possible to predict their future behavioral tendencies, making this information valuable in assessing whether a defendant is at risk of re-offending. Therefore, character evidence is widely used in traditional criminal proceedings. Character evidence can help

in understanding the psychological state of a crime suspect or defendant, including their motives, purposes, and intentions. Particularly in cases where direct evidence is lacking, it serves to assist in determining the truth of the matter and helps the court better understand the nature of the case and the causes of the criminal behavior. Character evidence, as auxiliary material for grasping the case, can help understand the suspect's lifestyle and moral character, thereby facilitating a better analysis of the case. Investigating character evidence can be done through various methods, such as interviews, conversations, psychological tests, and reviewing files. The investigation content also involves various aspects of the suspect's life, including basic personal information such as personal history, family situation, income level, social relationships, interests, life experiences, and their personality traits; social evaluations of the suspect, firsthand evaluations of their character and moral character by the suspect's relatives, friends, classmates, colleagues, neighbors, etc.; the suspect's previous criminal record and whether they have experienced various punishments, which is also an important measure to understand the suspect's character.

In certain types of cases, such as juvenile criminal cases, the application of character evidence is more common, as crimes involving sexual assault against minors often happen discreetly, with no witnesses present in many cases. Besides testimonial evidence, other types of evidence are often lacking. In such circumstances, it is important to focus on collecting evidence of the defendant's bad character in rape cases, as it can help in better understanding the situation and determining the facts of the case. Additionally, in these cases, character evidence may also be used to consider the rehabilitation potential of juvenile offenders and the ease or difficulty of their reintegration into society. Character evidence plays an important role in legal psychology, as it not only helps in understanding the psychological background of criminal behavior, but also plays a role in legal proceedings, assisting the courts in making more comprehensive and fair judgments. However, when using character evidence, it is also important to be mindful of the potential bias and unfairness it may bring, ensuring that it is reasonably applied while respecting individual privacy and rights.

Assessing behavioral patterns can help predict criminal motives and intentions in advance, and character evidence will also play a crucial role. In the cyberspace, by collecting and analyzing individuals' online behavioral records, evaluations, and feedback, their digital reputation can be established. Character evidence can to some extent reflect the reputation and historical behavioral patterns of individuals or organizations. This credit cost can increase the illegal costs for potential offenders, as misconduct may affect their overall reputation, thereby negatively impacting their future activities. The concept of character evidence can help members of society make wiser decisions when choosing partners, service providers, or engaging in transactions. An individual's character or reputation can be seen as a form of social capital, which can promote self-monitoring and mutual surveillance within a community, thereby reducing crime rates. At the legal level, character evidence can be used as one of the factors in judgment. In criminal proceedings, character evidence can be used to prove the character and consistent behavior of a criminal suspect or defendant, which is of great significance for the determination of facts and evidence review in a case. While the direct application of character evidence in criminal proceedings remains controversial, it can indirectly influence people's expectations and behavior. The existence of character evidence motivates individuals and organizations to maintain a good online behavioral record, as this directly relates to their status and opportunities in the online society. This incentive mechanism encourages people to abide by rules and laws in the online world, thereby helping to prevent cybercrime.

ii. Analysis of group psychology of online violence.

Last year, the Chinese police uncovered a case where criminals hired "internet water armies" to bully others online. In order to achieve long-term control over the victims, the criminals illegally

obtained the victims' privacy information by installing tracking and eavesdropping devices. They purchased internet accounts, hired "water army" groups to spread and hype up "indecent" videos, images, and insulting articles about the victims. They also sent false reports in the victims' name to their workplaces, leading to the victims suffering from post-traumatic stress disorder. Apart from intentional crimes, there are also many instances of deliberate and unintentional participation in online bullying by digital users in their internet activities.

In the online environment, individuals are easily influenced by the group. When they see others attacking or insulting someone or something, they may, out of the psychology of conformity, follow suit and participate, thus contributing to the occurrence of online violence. This phenomenon is particularly evident on social networking platforms, where irresponsible remarks and actions can trigger group violence online. Due to the fast spread and wide reach of information on these platforms, the psychological effect of conformity makes individuals more susceptible to the influence of others, thereby accelerating the spread of online violence. When a particular online violence event is widely shared and commented on, others may join the dissemination out of curiosity or the sheep mentality, causing online violence to spread rapidly. When a cyber violence incident receives a lot of attention and discussion, the victim may feel increased pressure and anxiety, and may even suffer from serious psychological trauma. On the other hand, the psychology of the bystander effect may lead individuals to increase their tolerance towards cyber violence, which in turn affects efforts to stop cyberbullying. When a cyber violence incident is widely publicized and discussed, some individuals may view it as a normal phenomenon or even believe that the victim brought it upon themselves, thereby weakening resistance against cyberbullying.

Moreover, there is a close relationship between collective unconscious psychological effects and the phenomenon of online violence. The anonymity and virtual nature of the online environment make it easy for individuals to experience collective unconscious psychological effects. When a group forms a common pattern of aggressive behavior, this pattern may continue to be reinforced, leading to an escalation of online violence and the emergence of overwhelming persecution. Victims may feel powerless to resist, resulting in further psychological pressure. Moreover, in this kind of collaborative aggressive behavior, members become more extreme in their average views when discussing a certain issue. In real life, people are often constrained by social norms, suppressing the desire to express extreme views. However, on the internet, individuals can make anonymous comments, which significantly reduces the psychological cost of expressing extreme opinions. When members of a group are all expressing extreme views, they tend to develop strong hostility towards those holding different opinions, thereby triggering online violence. At the same time, the immediacy of the internet also makes people more susceptible to emotional influence, leading to collective polarization. When someone is attacked online, they may become more steadfast in their own views and more opposed to other perspectives. This phenomenon is known as the "backfire effect," which can exacerbate the phenomenon of collective extremism.

People tend to feel sympathy and concern for individuals or groups who are vulnerable, injured, or treated unfairly. Therefore, when victims of cyberbullying are attacked or belittled online, they may become "the weak" and evoke the sympathy of others. This sympathy may result in people offering more support to the victims, helping them cope with cyberbullying. However, this sympathy can also be exploited, as some individuals may use others' compassion to gain attention or even benefits. On the other hand, the sympathy for the weaker effect may also exacerbate online violence. When someone is seen as a "weaker" individual, they may become easier targets for attacks. Some individuals may take advantage of this vulnerability to satisfy their own needs or elevate their status by targeting the "weaker" individual. Furthermore, even well-intentioned sympathy can unintentionally intensify online violence, as it may make the victim feel trapped in the label of "weaker," thus increasing their psychological burden.

The study of legal psychology can contribute solutions to the social issue of online violence. Through research in legal psychology, we can better understand the psychological mechanisms and impacts of online violence, thus enabling the development of more effective laws and regulations to prohibit and punish such behavior. This includes clearly defining the standards of online violence, establishing reasonable punishment measures, and implementing effective regulatory mechanisms. Through education in legal psychology, public awareness and understanding of online violence can be increased, making individuals aware of the dangers of online violence and how to protect their rights through legal means. At the same time, changing some people's misconceptions, such as thinking that cyberbullying is "not a big deal" or "not real", can also be achieved through public education. In addition to legal protection, victims of cyberbullying also need psychological support and help. Legal psychology can provide professional psychological counseling services to help victims deal with the negative emotions after experiencing cyberbullying, rebuild their confidence, and restore their normal lives. Legal psychology can also help us understand the factors that may lead to cyberbullying, in order to take preventive measures. For example, by improving people's social skills, educating them on how to handle conflicts and setbacks, we can reduce the occurrence of cyberbullying. This requires the collective efforts of governments, schools, communities, families, and individuals to build a healthy, friendly, respectful online environment.

4. Construction of Legal Legitimacy in Digital Society

The role that legal psychology can play in demonstrating the "legitimacy" of digital society laws should be to contribute to solving the proposition of how to re-establish a sense of belonging in a faithless digital society. Attitude determines behavior, "If a law is to be enforced, it must ensure its efficacy in social psychology... that is to say, the authorities that establish such laws must receive sufficient support from social psychological forces so that it can be effective even against individual resistance, and have the power to make the law an effective force for action. The effectiveness of law comes not only from the acknowledgment of the majority, but also from the specific binding and coercive force generated by the deep social foundations. It has already been transformed into a psychological constraint for everyone through social and cultural processes, which is a much more effective guarantee than tangible state violence. On the surface, it may seem that the enforcement of a law, especially national law, is ensured by external, particularly violent coercion. In reality, however, it is more sustained by long-established social customs and internalized social psychology. Assuming a person openly violates a law, for him, the most difficult is breaking through his own psychological defenses, followed by public condemnation, and finally the deterrent power of the law.

The online society and the real society share certain similarities, but also have many differences. Some common rules in the real society may not apply in the online society. The freedom, openness, anonymity, and spread of information in the online world determine the differences in legal construction between the online and real societies. Therefore, in online legislative activities, it is necessary to respect the laws of online development and grasp the basic properties of the internet in order for the law to truly fulfill its function. The digital society is a relationship sum of various forms of network communication activities participated in by humans. Some scholars believe that because the subjects on the internet appear in symbolic form, they naturally lose their essential human characteristics. That is, the internet space as a symbolic information repository actually determines that people's interactions in cyberspace are essentially symbolic interactions. This radical structuralist viewpoint clearly ignores the fact that the information conveyed in the form of symbolic interactions in online communication activities actually possesses spirituality, cultural characteristics, and social attributes. Although the viewpoint is biased, it correctly points out that the digital society is a world represented by symbols, and therefore, a part of the essence of the digital society is determined by the

characteristics of symbols. In attempting to construct a digital legal order that inspires conscious belief, it is necessary to align with the principles of psychological research. This is rooted in the scientific research methods of legal psychology, which can effectively observe the symbolic features of the digital society. Among the existing research tools, the use of psychological assessment analysis models can provide a scientific and quantitative analysis of digital behavior. For example, governing bodies can establish a hierarchical database for digital users, where users with lower levels of evaluation are restricted from using more advanced functions, such as individuals with alcohol abuse issues being unable to access autonomous driving features.

Conclusion

Currently, artificial intelligence technology has already replicated human knowledge, fundamentally changing traditional learning methods and causing unprecedented disruption to education. Digital skills, adaptability, and creativity will become the foundation for children's future success. Artificial intelligence has the potential to transform the human world into a dehumanized society, with technological progress advancing much faster than human adaptation. This may lead to a situation where technology does not serve human development, but rather humans must adapt to technology at the cost of their physical and mental well-being. Therefore, the study of human psychology plays an important role in preventing risks in the digital society, but based on the objective laws of the absence of individuals in the digital society, the key to building a digital legal regulatory approach may still lie in the improvement of scientific and technological means of supervision, as well as the logic behind the sophisticated procedural algorithms. Because the basis of law is justice, which belongs to subjective values, it is impossible to grasp justice based solely on personal intuition, external standards must be used. However, caution must be taken to prevent the emergence of algorithmic dictatorship. In the future, if the reasoning algorithms of the law are only formulated by a small number of people, the standard for judging justice is very likely to be distorted. If a few people dominate the rules of social operation with the help of artificial intelligence, then it is very likely to lead to the emergence of algorithmic autocracy, thus affecting the fairness and justice of the law.

References

Wang, F. (2013). *A Study on Citizen Online Participation in Public Policy Process*. Fudan University.

Gao, X., & Gao, S. (2014). Viewing participants in collective events from a social psychology perspective and their legal responses. *Frontiers*, Z9, 103–104.

Chen, Z. (2009). Issues of fact in judicial judgments: An examination from the perspective of legal psychology. *Application of Law*, 6, 44–47.

Le, G., & Li, A. (2012). Legal psychology: An applied discipline promoting judicial fairness. *Bulletin of the Chinese Academy of Sciences*, 27 (S1), 119–129.

Ma, A. (2010). A discussion on the basic theoretical issues of legal psychology. *Journal of Gansu Political Science and Law Institute,* 4, 51–59.

Xie, L. (2022). Formation and prevention of psychological control in telecommunications network fraud. *Journal of China Criminal Police College,* 1, 14–25. https://doi.org/10.14060/j.issn.2095-7939.2022.01.002

Wang, C., & Wang, Y. (2024). Analysis of the representation of psychological hidden damage of victims of telecommunications network fraud crimes and the research on the restoration path - based on NVivo qualitative analysis of 51 victim interview materials. *Journal of Zhejiang Police College*, 1, 91–110.

Jin, P., & Rui, B. (2011). "Embodiment Presence": A New Perspective on Research of Online Interaction. *Journalism and Communication Research*, 18 (05), 12–16+109.

Xu, Ya. (2024). Psychological research on social health and social governance. *People's Forum: Academic Frontiers*, 3, 94–103. https://doi.org/10.16619/j.cnki.rmltxsqy.2024.03.011

Zhang, D. (2013). Research on the phenomenon of online group polarization from the perspective of social psychology. *Journal of Beijing Police Academy*, 2, 36–38. https://doi.org/10.16478/j.CNKI.jbjpc.2013.02.002

Lu, J. (2012). The Psychological Basis of Legal Governance in the Social Transition Period: A Psychological Interpretation of the Social "Legal Order without Order" in the Transitional Period. *Journal of Lanzhou University (Social Sciences)*, 40 (3), 108–114. https://doi.org/10.13885/j.issn.1000-2804.2012.03.023

Информация об авторе

Боге Чжан – сотрудник Шанхайского высшего училища полиции Министерства общественной безопасности Китайской Народной Республики.

About the author

Boge Zhang – Employee of the Shanghai Police College of the Ministry of Public Security of the People's Republic of China, Shanghai.

Автор заявляет об отсутствии конфликта интересов.
The author declare no conflicts of interests.

Поступила в редакцию 27.04.2024
Одобрена после рецензирования 20.08.2024
Опубликована 28.12.2024

Submitted April 27, 2024
Approved after reviewing August 20, 2024
Accepted December 28, 2024