

From Dependency to Independence: On the Paradigm Transformation of Criminal Protection of Privacy Rights in China

Mengfan Zhang*

Department of Law, School of Public Administration, University of Electronic Science and Technology of China, Chengdu, 61000, People's Republic of China

**Corresponding author: Mengfan Zhang.*

Abstract

The extensive application of big data and artificial intelligence technologies has led to the ongoing erosion of privacy protection; however, the safeguards for the right to privacy under China's Criminal Law have clearly lagged behind. Judicial practice has relied on the crime of infringing upon citizens' personal information as the primary regulatory tool; however, privacy rights and personal information rights differ fundamentally in the legal interests they protect: the former protects personal dignity and the peace of one's life, while the latter upholds the order of information flow and self-determination. As evidenced by Guiding Case No. 265 of the Supreme People's Court and a number of representative cases of cyber violence, a considerable amount of conduct that directly undermines the dignity of privacy can only be prosecuted through the legal framework of personal information crimes, which creates a displacement in the evaluation of the protected legal interests. Meanwhile, the Civil Code has explicitly established the right to privacy as an independent and prioritized specific personality right, yet criminal legislation has consistently failed to establish dedicated provisions, leading to structural contradictions within the legal system. Through an analysis of legal interests and normative frameworks, this paper identifies three limitations in the current dependent protection model—regarding the evaluation of legal interests, the scope of protection, and constitutionality—and proposes the establishment of a “crime of infringement of citizens' right to privacy” to construct a dual-track paradigm combining direct and indirect protection. This transformation is not merely the addition of a new criminal offense but also a profound adjustment to the definition of legal interests, evaluation mechanisms, and systemic coordination, with the aim of providing comprehensive and effective criminal law safeguards for the right to privacy in the digital age.

Keywords

big data, right to privacy, right to personal information, dual-track system, crime of violating the personal information of the citizens

1. Introduction

The massive application of big data and artificial intelligence technologies has certainly altered the nature of the connection between the individual and the society. People as consumers, their health status and mobility patterns, as well as their social behavior, are continuously being turned into digital data that is further analyzed

by the algorithm to produce useful information resources. Privacy is gradually losing its position behind the screen of convenience provided by such technologies, and the uneasiness over the invasion of privacy is not just an imaginary concept anymore but a common concern in real life.

To address these crimes triggered by this phenomenon, the Chinese judiciary, basing its criminal practice on the crime of violation of individual privacy, has revealed a chain of contradictions over time: the meaning of the legal interests ensured by the right to privacy and by the right to personal information are substantially dissimilar. A criminal offense developed to maintain the order of information flow may also be displaced in itself to achieve the purpose of maintaining personal dignity. The invasion of personal information of a citizen, whether in the case of Wu** and Chen** [1] or in the case of Wang Qiang [2], in a criminal justice system, once the court determines that the actions constituted an invasion of the right to privacy of citizens, it is bound to restrict itself to the current roster of criminal offenses and thus forced to always categorize these acts as crimes that constitute infringement of the right to personal information of citizens. Nevertheless, the Personal Rights chapter of the Civil Code has already explicitly identified the right to privacy as one of the special and independent types of personal rights that must be prioritized. The difference between the protection of the right to privacy and the right to personal information has been expounded further by the Supreme People's Court in Guiding Case No. 265, the case of Luo *, a certain technology Co., Ltd., concerning the clash of the right to privacy and the protection of personal information, which says that even when the act of collecting user profiling data might be viewed as a breach of the rights to personal information, they should be viewed separately in contrast to the breaches of the right to privacy. Such disparity in which the legislative advancement has made great steps forward, but criminal law security lags far behind is still a dilemma that should be resolved immediately.

The right to privacy is one of the basic rights of individuals, and it should not be understood solely as the right to personal information under criminal law. Rather, it must turn the indirect safeguard into a dualistic system that is comprised of both direct and indirect safeguards, which is more than the implementation of new criminal laws but is rather the change of the concept of legal interest, the assessment systems, and the systematic integration. The present study will begin with the examination of the limits of the legal interests protected by the right to privacy and the right to personal information, the drawbacks of the current dependent protection model, and the threats to the constitutionality it poses, lastly, the research will provide the suggestion of a systemic restructuring model that will aim to introduce an offense of the violation of the citizens' right to privacy.

2. The Erosion of Privacy Protection in the Big Data Era

2.1 The Trend Towards the Over-expansive Application of the Crime of Infringing Upon Citizens' Personal Information

The invasion of personal data of citizens has turned into an international phenomenon in the modern criminal justice system. It starts with professional underworlds that conduct illegal trade in massive amounts of personal information of citizens, then it proceeds to individuals who place miniature cameras in hotel rooms in order to covertly film other individuals and extends to other individuals who use web scraping technology to obtain contact information of corporate legal representatives online and sell the info to others; despite the fact that these two groups can be extremely different depending on their targets, their methods as well as the damage they cause to society, they often wind up being categorized as one crime.

In the criminal case of Wu **, Chen **, et al. (Case No. (2020) Su 0508 Criminal 714), which is an example of online violence, the criminals got the personal information of their victims through the unlawful approaches of doxxing and subsequently published defamatory content regarding the victims online with the total number of views and reposts reaching over 2 million. Subsequently, the court finally convicted and sentenced the accused individual to the charge of infringement of the personal information of citizens as per the provision concerning the other serious conditions specified in the judicial interpretation. Moreover, in the case of Wang Qiang, who had violated the privacy of citizens (Case No. (2020) Qian 04 Criminal Appeal 155), various offenders utilized a personalized data scraper tool and a super administrator account and password to which they had access to the Good Data online lending traffic generation system to scrape personal information of citizens over the internet and then sell it to others for a profit. It was made clear in the judgment in the appeal

that what the perpetrators did in infringing upon the personal information of citizens also violated the right to privacy of citizens. Nonetheless, the problem of privacy rights was only raised during the supplemental civil lawsuit and accused of the identical crime of breaking the privacy of citizens' information.

The general view of the cases that can also be regarded as a catch-all solution can be seen as adding to the efficiency of courts, but it hides a major problem. The core of the crime of violating the personal information of the population is to regulate the flow of information and individual rights to have access to their own information, but the main harm caused by the violation of privacy is the personal damage to the internal peace and dignity of a human being. In case a person experienced the private body exposure, spatial movements, or the private talks of other people and this happened without the permission of the person involved the purpose of this attack would be the degradation of personal dignity and the collapse of the inner feeling of order in the person - not just loss of control over information. It is like weighing the weight with the help of a thermometer as the attempt to quantify this qualitative infringement of personal dignity with quantitative measures, i.e., the total volume of information, or even illegal profits: the measure is wrong compared to the thing to be measured. This bias in the assessment of the law interest has been institutionalized and extended due to the long-term judicial inactivity, which can eventually lead to the death of the idea of basic fairness in the creation of criminal responsibility regardless of the guise of exact criminal liability and punishment [3].

2.2 The Mismatch Between Independent Protection under Civil Law and Supplementary Protection under Criminal Law

Privacy is a right that is currently recognized by legislation. There is a stark discrepancy between the manner of protecting privacy in civil society and the manner of protecting privacy in criminal law, where privacy protection is subsumed under the cover of other criminal offences. In sections, the Personal Rights sections of the Civil Code list consecutive chapters to the right to privacy and the protection of personal information. This contrast alone is a very strong normative message: despite being very close, they are disconnected regarding the legal interests that they protect and the rules of protection that they have. Most importantly, civil law has also developed laws to address conflicts between them. Article 1034, paragraph 3 of the Civil Code is very clear in stating that when a piece of information possesses both the quality of personal information (identifiability) and the quality of the privacy of the personal life, the law gives precedence to applying the rules of privacy protection and the rules of personal information protection are only applied as supplementary measures [4], which means that the hierarchy of values of civil law places the right to privacy higher up on the list of fundamental and prioritized legal interests. Moreover, according to the Interim Provisions on Disclosure of Complaints by the Market Supervision and Administration, the release of complaint information to the public should also be agreed upon by the consumer and it should not expose sensitive information about personal privacy; Article 1 of the Provisions of the Supreme People's Court on Certain Issues on the Application of the Law in the Civil Cases of Infringement of Personal Rights by Information Networks states directly: Civil cases of infringements of personal rights by information networks, referred to in this provision, mean those civil cases caused by the infringement of another person's personal rights, such as the right to a name, right to a trade name, right to reputation, right to honor, right to one's likeness, and right to privacy by information networks; Article 2 of the Regulations on the Protection of Minorities in Beijing stipulates: Ensure the privacy rights of minors and their personal data... There are a series of laws and regulations that specifically focus on the protection of personal privacy as opposed to the ambiguous concept of personal information.

It is clear that the legal system has an inherent unity, and therefore, it would be right to say that the different branches of law should cover similar types of legal interests in about the same way. Nevertheless, the concept of privacy is not explicitly mentioned as part of the Criminal Code concerning criminal law; it can only be guaranteed by twisting the criminal laws or basing its existence on the body of criminal offences, including the crime of revealing information relating to citizens, the crime of illegal intrusion into a flat, and defamation. It is shocking to see that only 48,656 criminal cases are found when using the keyword of privacy to search judicial cases in the database of the Peking University Law, which is much less than 307,899 civil cases. In the opinion of the Supreme People's Court entitled Six Typical Cases of Infringement on Personality Rights Using Internet and Information Technology, illegal access to the control of smart home devices is an excessive infringement of the right of people to privacy and protection of their private information, which suggests that in reality, courts have already reached the understanding that personal privacy and personal information can

be treated as two different legal interests and that criminal law has always been lacking particular protective regulations concerning the right to privacy. A contrary case, where civil law has taken a very high level of independence and criminal law has greatly lagged behind, cannot be viewed as a reasonable structural contradiction in the legal system.

2.3 The Independent Value of Criminal Protection of the Right to Privacy

The observations mentioned above, based on judicial and normative views, lead to one general conclusion: that privacy as a human right should be provided with a separate and non-substitutable position in criminal law. The problem is that the existing criminal law does not provide protection of privacy, but this protection will not take place unless it is based on other parts of the law. To illustrate, unlawful invasions of homes are covered by the peace of the home, insults to social reputation, and attacks on the personal information of citizens by the right to informational self-determination or information security order. Even though these legal interests are very closely connected to the rights of privacy and can overlap in terms of protection in particular cases, all of them cannot fully and accurately cover the special character of unlawful privacy violations.

Article 3 of China's Law on Public Security Administration Punishments also leaves legislative room to protect the right to privacy using criminal law. "If any of the personal rights, including the right to privacy, are violated, it should be as follows: if these actions are criminal offenses under the Criminal Code of the People's Republic of China, criminal responsibility shall be imposed by law; otherwise, administrative punishments must be administered to them under this Law by the police." [5] This implies that when someone greatly violates the personal privacy of another individual, there is no way to punish such a violation with just one administrative measure, and criminal law is required to plug this loophole. There is an idea of a personal life not being intruded upon and a personal area not being spied upon that is an independent interest which ought to be safeguarded by criminal law rather than being considered as a derivative of other rights or an incidental consequence of protecting them [3]. To solve this problem in reality, it is supposed to begin with the creation of the legal environment of independence in the right to privacy, since only thereafter any further institutionalization would have a sufficient basis.

3. Distinguishing the Legal Interests of the Right to Privacy and the Right to Personal Information

3.1 The Right to Privacy: "Negative Liberty" Grounded in Human Dignity

Privacy as a right is the establishment of a personal space in a person where outsiders can be allowed to interfere to a minimal degree. It has the quality of privacy as the central element and has various dimensions, such as the peace of private life, private areas, private actions, and private data. The final aim of this protection is the individual himself, that is, his/her honor and desire to grow and form the character in this very atmosphere where it is not interrupted [6].

The reason why this right can be viewed as a practical issue is that of passive protection; the rights holder is not required to act but allowed the space to inform the other people in the world that they should leave the rights holder alone. Privacy in the digital age is taking different shapes, but its meaning remains the same. By integrating the fragmented data, which are the history of the web browser, consumption patterns, and social interactions of a particular individual, algorithms may build extremely personal profiles that are sensitive in nature. The derived information could be more precise and close to the data that the rights holder has purposely given. Such derived privacy data keep on attacking the person who does not want to be examined by the eye of technology - they hit the core of his personality [7]. The shift in environmental conditions brought by technological innovations does not lead to the loss of the right to privacy independence, it needs to be expanded to cover the emergent types of invasion.

3.2 The Right to Personal Information: "Active Control" Based on Data Circulation

In contrast to the right to privacy, the main feature of the right to personal information is substantially different since it is based on the concept of information identifiability, i.e., the possibility of identifying and locating one particular natural person in a population by using certain information and should be treated as one of the kinds of individual civil rights [8]. The right is not to imply that the information must be a secret but

that the person with the right can choose to make independent decisions and positively manage information that might be used to identify them, such as the sovereignty over the entire life cycle of the information, which includes the gathering, holding, and use through the processing, transfer, provision, and disclosure of the information [9].

The object of protection under the right to personal information possesses an inherent dual nature. On the one side, it protects personal interests, and information leakage and abuse may cause a sequence of violations of personal safety, property, and in some cases even personal dignity. On the other side, it also protects property interests and the common good since smart information circulation and exchange help to facilitate the sound development of the digital economy; otherwise, this will increase the negative externalities of digital technology on social governance and individual rights. The result would be that the institutional structure of personal information rights needs to be balanced along the lines of protection and control and exclusivity and sharing. Any social media profile created by an individual which is no longer private is also part of personal information rights as it is identifiable and is not a form of public information which can be accessed randomly. It indicates the main issues of the right to personal information and the right to privacy, taking different paths since they were created: the first one is about who holds the power over information, and the second one is about what information should be hidden.

3.3 The Dual Nature of Private Information and the Attribution of Legal Interests

Privacy and the right to personal information are not two separate and non-related concepts, but rather are combined into the notion of what is sometimes called private information. Medical and health records, sexual orientation records, religious beliefs records, financial account passwords records, etc. share these properties: identifiability, i.e., the ability to use them to identify a particular person, and privacy, i.e., the sensitivity of the content because they contain highly sensitive information, which is frequently the boundary between these rights.

As concerns the essence of this gray area, the official position is expressed clearly and confidently: the legislation on the right to privacy is more important. The civil law has already established enough of the normative ground on this bias; the legal justification of this rationality of prioritization is the fact that human dignity is more important than the order of use and distribution of information. It ought to be extrapolated to criminal law in these contexts: when a criminal is purchasing, selling, or revealing other people's information improperly, the criminal law should start by disregarding the amount of information sold by the criminal or the amount of money he/she made and instead consider the level of damage and seriousness of the damage caused by the criminal actions to the individual dignity of the data subject. One of the mechanisms that might serve as a perfect illustration of such an evaluative role is the case of a standalone crime of invading privacy.

3.4 The Personal Information Framework Cannot Comprehensively Protect Privacy

Privacy and personal information intersect in the sense of exclusion. Because the model of personal data protection is based on the idea that identifiability may be just a few conditions, or perhaps even the only condition, it does not address all the aspects associated with privacy rights.

It has become apparent that there are huge volumes of private information which could not be seen as information as they were part of a typical day. The dynamism of private actions, the privacy of the private environment, and spoken utterances in the course of private discourse are what form the core of the right to privacy, not necessarily that they should be kept on a computer or in any other way and not necessarily that they should be identifiable to a particular person. This may be stated as a hotel room, but it is not possible to describe in what manner the human dignity can be violated in this hotel room when the spy activity takes place in terms of recognizability. The creators of the Criminal Code in Germany have definitely understood such a differentiation between the targets of protection. They have laid down, in Chapter 15, different offenses of intrusive behavior in personal space including specific prohibitions concerning photographing individuals in the home or in very secluded spaces or different punishments in the presence of recording or listening to private conversations. These legislative instances indicate that in addition to the sphere of information, there is also another sphere of privacy, namely space and activity, that also needs separate elements of crime to protect them.

4. Limitations and Crises of the Current “Dependent” Protection Model

4.1 The Shift from “Personal Rights” to “Rights to Public Order”

It should be mentioned that the distinction between personal information and personal privacy was already present in Chinese civil law and administrative law. According to the principle of unity of the legal order, criminal law must also distinguish between personal privacy and personal information, rather than confusing them. The most serious consequence of such a view on conduct that violates the privacy as a crime of violating the population's personal information is the substitution of the legal interests related to the right to privacy with the ones related to the right to personal information as part of their assessment by the law in the process inadvertently.

It is discussed in the criminal law literature whether there are specific legal interests that are protected by the crime of infringing on citizens' personal information or not, but two theories, the right to informational self-determination theory, which builds on individual legal interests, and the information security order theory, which builds on supra-individual legal interests, treat the issue of information circulation as such. The first instance is when a person sees the fact that he has lost the control over the information, and the second case is when a person sees the fact that the balance between the information order has been upset. According to the people who oppose this sentence, this law defends the legal interests of the group due to the fact that it is not just about one person but also about the benefit to all people and sometimes the safety to the country [10]. Nevertheless, the one thing that is beyond dispute is that none of these legal interest ideas can adequately represent the actual pain points of privacy violations, i.e., that stabbing of personal dignity, that unrest of inner peace, and that feeling of humiliation that takes place when someone is forcefully intruded upon their private space.

The fact that a camera is present in the bedroom of a person and that this video is not shared with others publicly is not considered to be a disorder in the information flow order, and it may even be ignored as an offense of infringement of the information of citizens because the illegal acquisition, sale or delivery of such information is missing. Nevertheless, it is a very serious infringement of the right to privacy and leads to irreparable psychological damage to the victim. In these circumstances, the existing Criminal Law will either leave the jury deadlocked due to its inability to determine whether there were any proper charges they could have brought against them, or it will leave it biased as they were forced to bring other charges. Regardless of how it is presented, it reveals the excessive malfunctioning of the concept of dependent protection in the realm of legal interest evaluation.

4.2 The Exclusion of Pure Privacy under the “Identifiability” Standard

Identifiability acts as a necessary part of invading the privacy of citizens by criminalizing their personal data. The stated threshold is used as a filtering mechanism to reduce the identity theft and the illicit sale of information but simultaneously it erases the majority of unlawful intrusions into privacy that are not addressed by the criminal law.

The common scenario is to invade a person and their activities. As a particular case, placing hidden cameras in other people's homes, hotel rooms, changing rooms, or bathrooms (as long as the assailant is not recording but merely watching the view) could not be viewed as an illegal invasion of private information without significant difficulty. There is a legal loophole in the criminal law because no individual has been identified, and no data is being entered. Currently, artificial intelligence technology development is becoming even more relevant: the large language models may process and generalize very large volumes of information that are originally completely non-identifiable and provide extremely sensitive personal profiles. These assumptions have done damage since they involve very personal information instead of the fact that the initial information is identifiable [11]. When this happens, traditional guidelines almost cease to be effective, and it results in a terrifying result: the criminal law safeguards the data formats marked as identifiable (that is, the form) but fails to cover the real impact of the breach of privacy.

4.3 Non-compliance with the “Principle Prohibiting Insufficient Protection”

This is evident in most of the dilemmas highlighted above on the level of the substantive law, but it is not just a mistake in the criminal law doctrine, but it causes extremely serious issues on the constitutional plane

regarding the responsibility of the state to protect. Fundamental rights are understood by the state as not only a negative non-intervention duty but also a positive duty to ensure protection. It is necessary to ensure the functioning of the institutional guarantees of the implementation of fundamental rights through different mechanisms: legislative, judicial, and executive. Such a state-based responsibility of protection is not unlimited; its constitutional monitoring system is the concept of insufficient protection. According to this concept, the protective measures taken by the legislature in order to protect fundamental rights should have a certain degree of effectiveness; they should not be just an announcement or ceremony, but must involve real constraints on possible violators, and consequently, overall, a minimal level of protection of fundamental rights [12]. If the impact of technology on privacy becomes particularly acute (in such cases when the use of civil remedies is ineffective and the administrative liability is insufficient) the inability of the state to meet its positive obligation to create criminal laws may be viewed as an infringement upon the positive obligation of the state to protect human dignity as stipulated in Article 38 [13] and Article 40 [14] of the Constitution and thus is a violation of the principle of insufficient protection.

The use of this criterion in the evaluation of the right to privacy protection by means of the existing Criminal Code reveals that, in terms of formality, the entire Code does not contain any specific articles or offenses relating to the right to privacy, thereby rendering it rather inconspicuous. Actually, most of the intrusion of privacy that results in serious psychological damage is not chargeable as a crime (it cannot be defined as an invasion of privacy because it does not have the characteristic of identifiability or it cannot be defined under the existing types of offenses) and therefore, the need to turn to civil damages and administrative penalties as the last resort is created and thus, a criminal accountability gap is formed. The fact that the criminal law is clearly lacking in all the major areas of its functioning when it comes to the protection of fundamental rights makes it reasonable to consider carefully whether the protection offered by the laws still corresponds to the minimal requirements of the Constitution. It is exactly in this context that the statement that can be found in this article is formulated: a change should be implemented at the level of the legislative theory.

5. Constructing a Dual-Track Model for the Criminal Protection of Privacy Rights

5.1 The Necessity and Feasibility of Introducing the Crime of Infringing Upon Citizens' Privacy Rights

In order to break the existing impasse, it is necessary to alter the traditional attitude that considers the right to privacy as subordinate to other rights and provide the direct safety by creating a personalised offense of violation of the right to privacy of citizens.

Privacy is a legal interest that is independent; the subject matter of peace of mind, private space, private life, and confidential data that it protects are a group of interrelated interests that cannot be replaced by any other legal interests. Despite the fact that there could be some resemblance between the right to privacy and the right to personal information, essentially they cover different spheres of protection. The control gives the cause to shield personal information but the secrecy and calmness give the cause to shield the right to privacy. This inconsistency in the character of the legal interests indicates that the first cannot completely displace the second one [6]. Criminal offenses against individual privacy and the private sphere [15], including the violation of privacy of speech and the invasion of individual privacy and personality rights through photography or other pictures, etc., are included in the list of crimes against privacy in the German Criminal Code, Article 15. This law also shows that the criminal offense system may be unified and strict, when it comes to the successful introduction of the offenses against the private life and the secrecy zone into an integrated and consistent criminal offense system, offering selective and direct protection to different types of privacy, such as the private space, private conversations, and private images. These are not mere hypotheses but practical solutions that have successfully stood up to judicial review because of their capacity to withstand judicial review. In reality, the extent of the new crime is unequivocally clear and unambiguous: it is exactly meant to cover the infringement of privacy without having recourse to the existing crimes that are incompetent to cover the infringement. It also creates a companion and supplemental relationship with the crime of intruding on the personal data of citizens, which does not mean the vagueness of the statutory correspondence, but enhances the degree of completeness and complexity of the protection system.

5.2 Clarifying the Threshold for Criminal Liability Regarding Private Spaces, Activities, and Information

Not only does a single criminal act have relevance because it was reported, but also because it gives the judge an unmistakable and functional list of factors, which he or she can consider in his or her job. The novel crime of Invasion of Citizens' Right to Privacy should be incorporated into Chapter 4 of the special section of the Criminal Law, that is to say, Crimes against the Personal Rights of Citizens and their Democratic Rights. This is all about securing the personal rights of people, and its position in the legal system will be determined by what type of legal interest the new offense protects.

To determine the offense, it may be useful to take into account three aspects of parallelism in a core structure, namely: private space, private action, and private information. The main components of the offense are: illegal access to, intrusion into, shooting of, filming of, or any other invasion of another person's private space or activities; and illegal accumulation, manipulation, sharing, distribution, or provision of another person's private information to other people. As all these three categories are considered to be protected objects to the same extent, the offense includes all privacy rights so that the loopholes in the existing legal framework in terms of what can be referred to as non-information-based privacy and violation of privacy without spreading information are filled [16].

The separation between the serious situations and the criminal responsibility is one of the fundamental guarantees of the principle of restraint in the criminal legislation. The conditions of this border must be not just different than those of the quantitative approach, which is aimed at the volume of information and illegal benefits, i.e., infringement of personal information of citizens, but they must also be different than the administrative penalties set out in Article 50, Clause 6 of China's Law on Public Security Administration Punishments [17]. Administrative offenses are offences that have individual, specific and material characteristics and are committed in the private sphere, but the criminal offence of violating the right to privacy of the citizen should include harassing privacy through online and media outlets with the help of modern information technologies and technologies, focusing on the practical effect of the conduct on the dignity of the victim, state of mind, and emotional health of the victim. Serious circumstances should be determined considering such important factors as the level of intrusiveness of the methods used, the frequency and frequency of the infringing actions, the extent of dissemination, whether the victim underwent serious psychological repercussions or even committed suicide because of it, or if the methods used were particularly dehumanizing to the dignity of the victim and had negative social repercussions on him/her during his lifetime. This hierarchical model of evaluation that relies on harm to personal dignity does indeed represent the natural harm caused by privacy violations and is an important step in shifting the evaluation to the essence [18].

5.3 The Rule of Concurrent Offenses Between the New Offense and the "Crime of Invasion of Citizens' Personal Information"

The dual-track protection system needs to have a clear structure so that neither of the violations could induce another level of confusion in practice.

In case an act also turns out to be unlawful in respect of two legal interests, it is recommended to view it through the prism of imaginary concurrence. For instance, imagine that a perpetrator purchases and sells a large amount of medical records that contain very detailed medical history, genetic information, and sexual preferences of other people. This is extremely sensitive personal data which has the properties of identity of personal information and privacy protection. It is a breach of the right to informational self-determination and the right to privacy and should be punished more severely to ensure that the overall negative assessment of such mass compound crimes is right.

In case an act involves only one legal interest, the difference between these two offences can be quite easily determined. The act of merely looking into a hotel room might also be penalized as an offense of invasion of the privacy of a resident; the act of simply printing non-private information of another person, which had been obtained legally, might also be penalized as an offense of invasion of the personal data of a resident. These two crimes do not influence one another, but allow evaluating the violation of various types and levels of legal interests in different and accurate ways [19]. Such an approach, which could be defined as well-defined separation of duties and systematic coordination, is actually the structural benefit of the dual system over the single and interconnected one.

5.4 Complementary Defense Mechanisms under the Dual-Track System

Also, it should be noted that before the independent legislation is completed, it would be better to protect some types of personal data (which are in the grey zone) indirectly with the help of judicial interpretation, which would serve as the institutional safety net in the creation of new criminal offenses. As an example, it would be reasonable and feasible to modify the definition of the concept of the personal information of citizens in the context of the current judicial interpretations to a much more practical concept of privacy.

To be more exact, one could suggest using an integrative evaluation standard that would involve incorporating the two concepts of weak identifiability and privacy into it. There are some kinds of information that cannot be regarded as indicating a particular person directly but can still be categorized as personal information protection because the combination of that information with any other technical means or situational factors will probably identify a specific person, and the nature of this information is so private that its presence is expected by each member of society. One instance of this scenario can be observed in the medical sector in which medical records are highly confidential and once they are disclosed they could inflict significant damage to the individual's rights. Although these pieces of information are already partially de-identified, criminal law must treat them as equally important because of the higher probability of privacy violation risks [20]. This interpretative approach is valuable because it offers a solution to multilayered protection of privacy that can be achieved by improving the court practice without substantially changing the Criminal Law articles.

6. Conclusion

Privacy is the ultimate barrier of human dignity. The individual finds himself in a new dilemma of openness on this very day, when digital technology has entered the lives of each person, and algorithms are silently rearranging the social order. The borders of personal space have completely altered with the massive gathering of information, constant profiling of users, and advanced intrusion systems whereby an invasion is now a kind of erosion.

Criminal legislation of China opted to include privacy among the areas of protection of personal information and other criminal offenses. Although this dependent system has maintained the formal efficacy of reducing crime during a short time, it is by nature susceptible to defects, such as the misalignment between the evaluation of legal interests and the narrowness of their protection, and can be observed as a legitimacy crisis due to the constitutional duty to protect the fundamental rights. It is evident under the current conditions that the right to privacy should be recognized in civil law and personality rights should be accepted, but also in practice and incorporated in criminal law as the final form of protection, where it ought to be regarded as a separate kind of legal interest that is provided with specific criminal protection.

The paradigm shift in the relationship between dependence and independence does not lie in the mere addition of another crime to the list of crimes, but rather in the termination of conceptual renewal and reorientation in relation to the position of the right to privacy in the criminal law. It has become an instant response of criminal laws to the autonomous value of the right to privacy as codified in the Civil Code, and the structural vulnerability of criminal law to the most intimate freedoms and dignity of a person when there is a sharp rise in the strength of information. The only way criminal law can really be effective in making sure major breaches of privacy are not evading the law is by adopting a dual track approach that includes direct and indirect protection and at the same time creating enough institutional space to innovate in technology and information flow in the era of big data.

References

- [1] Criminal Judgment of the People's Court of Gusu District, Suzhou City, Jiangsu Province (2020) Su 0508 Criminal No. 714.
- [2] Criminal Judgment of the Intermediate People's Court of Anshun City, Guizhou Province (2020) Qian 04 Criminal Appeal No. 155.
- [3] Wei Chen, Yucen Wu. (2024). The Reconstruction of Criminal Law Protection Mode of Privacy in the Big Data Age. *Journal of Southwest University of Political Science & Law*, 26 (1), 107-121+162.

- [4] Article 1034 of the Civil Code, <https://xcx2019.faxin.cn/m/v5/web/twsy/TwsyContent.aspx?isapp=1&gid=A290592&twsygid=47878&tiao=1034>.
- [5] Article 3 of the Law of the People's Republic of China on Public Security Administration Punishments.
- [6] Liming Wang. (2013). Legal Protection of Personal Information: Centered on the Line between Personal Information and Privacy. *Modern Law Science*, 35 (4), 62-72.
- [7] Xianquan Liu. (2025). The Criminal Law Protection of Citizens' Privacy Rights in the Era of Artificial Intelligence. *The Jurist*, (5), 15-26+190-191.
- [8] Yongqiang Ma. (2021). On the Confirmation of the Legal Interest Attribute of the Crime of Infringing upon Citizens' Personal Information. *Global Law Review*, 43 (2), 102-118.
- [9] Guangquan Zhou. (2021). On the Object of the Act in the Crime of Infringing upon Citizens' Personal Information. *Tsinghua University Law Journal*, 15 (3), 25-40.
- [10] Xinjiu Qu. (2015). On the Supra-individual Legal Interest Attribute of the Crime of Infringing upon Citizens' Personal Information. *People's Procuratorial Semimonthly*, (11), 5-9.
- [11] Chuankai Guo. (2024). Reflection and Reconstruction of Sensitive Personal Information Processing Rules. *Tribune of Political Science and Law*, 42 (3), 102-113.
- [12] Zheng Chen. (2021). On the Principle of Prohibition of Under-protection in the Constitution: A Comparative Study with the Principle of Proportionality. *Chinese Journal of Law*, 43 (4), 55-72.
- [13] Article 38 of the Constitution of the People's Republic of China.
- [14] Article 40 of the Constitution of the People's Republic of China.
- [15] German Civil Code, Division 15, Violation of the privacy of personal and private sphere, German Criminal Code, https://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html#p1939.
- [16] Benqi Ouyang. (2021). Redefining the Legal Interests in Criminalization of the Infringement of Citizens' Personal Information: A Shift from Private Law Rights to Public Law Rights. *Journal of Comparative Law*, (3), 55-68.
- [17] Article 50(6) of the Public Security Administration Punishment Law.
- [18] Tong Zhao. (2024). Layered criminal law protection of personal information in the dual structure of legal interests. *Journal of Southeast University (Philosophy and Social Science)*, 26 (4), 87-97+151.
- [19] Bo Xiong. (2023). Criminal Protection of Data Classification and Grading. *Tribune of Political Science and Law*, 41 (3), 155-167.
- [20] Xiaohong Guo. (2025). Criminal Law Characterization of Medical Data Breach: Disputes and Solutions. *Law Science*, (10), 98-113.

Funding

This research received no external funding.

Conflicts of Interest

The authors declare no conflict of interest.

Acknowledgment

This paper is an output of the science project.

Copyrights

Copyright for this article is retained by the author (s), with first publication rights granted to the journal. This is an open-access article distributed under the terms and conditions of the Creative Commons Attribution license (<http://creativecommons.org/licenses/by/4.0/>).