Humanities & Social Sciences Communications

ARTICLE

https://doi.org/10.1057/s41599-025-05141-y OPEN

# Criminalisation of the illegal use of personal data: comparative approaches and the Chinese choice

Zhilong Guo[1]✉

Different jurisdictions have different criminal law attitudes towards the illegal use of personal information, i.e., no criminalisation, selective criminalisation based on specific conditions, or overall criminalisation. China should move from the first approach to a new approach. China's criminal law has adopted a traditional privacy protection strategy focusing on information transfer. The existing crime of infringing on citizens' personal information is limited to addressing the illegal acquisition and provision of personal information. Nevertheless, it fails to fully consider the core position of the right to use in the full life cycle of the autonomous operation of personal information. By doctrinal analysis, the urgent and precise risk of further damage to citizens' personal lives, property, and social order contained in illegal use provides a solid basis for criminal law regulation. According to policy analysis, in jurisdictions where information technology such as big data and AI is widely available, for example, China, the illegal use of personal data particularly disrupts the community's sense of security. Criminal law should expand its scope, but it must justify its reach. On the one hand, by categorizing the illegal use of personal information, a comprehensive judgement can be made about whether to criminalise certain behaviours according to the degree of infringement on personal information autonomy, the harm to other legal interests, and the level of personal danger posed by the perpetrator. On the other hand, the corresponding reasons for exceptional noncriminalisation should be determined in the respective private, personal, and social spheres to achieve a balance between protecting citizens' autonomy in using personal information and highlighting the value of data circulation. This investigation process and the results can serve as references for member states of the GDPR and other jurisdictions seeking more rigorous protection of personal data in contemporary society.

[1] China University of Political Science and Law, Beijing, China. ✉email: fadaguozhilong@163.com

## Introduction

A decade ago, De Hert asserted that the drafted European General Data Protection Regulation (GDPR)[1] was unwilling to coordinate civil compensation, administrative, and criminal sanctions and that this unwillingness is appalling and indefensible (De Hert 2014). The coordination of different sanctions in the GDPR framework has not been updated. Although criminal sanctions are necessary and feasible within a jurisdiction, they are coordinated with administrative sanctions and civil law sanctions (Dimitrova 2019, 2020; Shutova 2022). The second part of this paper shows that, over the past decade, various jurisdictions have made specific assessments and choices concerning the criminalisation of illegal acts, especially the illegal use of personal data,[2] with different approaches and to different degrees according to their respective legal systems, criminalisation needs, cultures and theories of personal data protection. The GDPR is retained in domestic law as the UK GDPR is, but the UK independently reviews the framework. The second part analyses how the UK chooses not to directly criminalise the illegal use of personal data, whereas Germany, as a member state of the GDPR, chooses to criminalise it.

In recent years, Chinese scholars have discussed the criminalisation of the illegal use of personal information and agreed on the necessity and feasibility of criminalising the illegal use of personal information (Liu 2019; Liu 2020; Liu and Song 2022; Lu and Zhang 2023). However, there are still large differences in the conditions under which the use of personal information is criminalised (whether and how to specify the types of behaviour and determine the degree of illegality of the use of personal information) and the degree of criminalisation (how to determine the legalization of the use of personal information and the range of legal penalties). Therefore, this article aims to conduct a systematic study on the criminalisation of the illegal use of personal information by comparing criminalisation models and summarizing key criminalisation issues (Part 3); considering the current situation and trend of China's personal data legal system, practices, principles, and needs of criminal legislation (Parts 4 and 5); and showing how a specific jurisdiction such as China can improve its criminal protection system concerning personal data (Part 6). This investigation process and the results can be useful to member states of the GDPR and other jurisdictions seeking intensified protection of personal data in contemporary society.

## Key definitions and theoretical context

**Key definitions**. Before beginning a formal study on the criminalisation of the illegal use of personal information, it is necessary to define the illegal use of personal information. The definition of personal data can differ across jurisdictions and is not the focus of this study. For the purposes of this article, it is sufficient to cite the definition of personal information specified in current Chinese law. Article 4(1) of the 2021 Personal Information Protection Law (PIPL) stipulates that personal information is information related to identified or identifiable natural persons recorded electronically or by other means, excluding information that has been anonymized.

Thus, we should seek a technical and legal definition of the possible uses of personal data. China's PIPL does not define the use of personal information but only lists it as one of the ways personal information is processed in Article 4, paragraph 2. Article 3.6 of the 2019 departmental normative standard, 'Internet Personal Information Security Protection Guide', issued by the Network Security Bureau of the Ministry of Public Security jointly with the Beijing Network Industry Association and the Third Research Institute of the Ministry of Public Security, defines the use of personal information as any operation involving personal data by automated or manual means. These operations include recording, organizing, storing, adapting, retrieving, consulting, disclosing, disseminating, providing, adjusting, combining, restricting, deleting, etc.

However, this broad definition has been difficult to apply after the 2021 PIPL (Article 4, paragraph 2), which distinguishes the use of personal information from the collection, storage, processing, provision, disclosure, and deletion of personal information and lists them all as specific processing methods. We therefore follow the more authoritative rule of the 2021 PIPL. According to this rule, the use is different from the provision, such as selling. Correspondingly, the Explanations of Common Terms in the Data Field (Second batch) published in 2025 by the Chinese National Bureau of Data state the following: "Generally, the right of use is the right of the right holder to use the data for internal use without providing the data to the outside world." Specifically, Article 7 of the national standard 'Personal Information Security Code' (GB/T 35273–2020) lists the use scenarios of personal information, including the display of personal information, the use of user portraits, the use of personalized displays, the convergence of personal information collected for different business purposes, the use of automatic decision-making mechanisms of information systems, etc. as specific types of personal information use. However, from this list, it is still difficult to extract a unified and clear definition.

The definition of 'personal information' in the Personal Information Protection Act can help us clarify the definition of the use of personal information to a certain extent. Article 4(1) of the PIPL stipulates that personal information is related to identified or identifiable natural persons. Therefore, the 'use of personal information' as the object of this study refers to the behaviour of directly exerting the effects of various information related to identified or identifiable natural persons, which directly determines the subject, object, time, method, occasion, and purpose of exerting the effects. It refers to the personal information controller/processor's management and operation of personal information after collection, processing, polymerization, and analysis. Therefore, it has a particular purpose for fulfilling a particular function or service, particularly to optimize production and operation, form derivative data, etc. For example, creating a personal portrait or making a decision on the basis solely of the automated processing of personal information, which may have legal or other significant effects on the information subject, is a typical use of personal information (Fan 2023). Under normal circumstances, sales, exchange, disclosure, retrieval, consultation, disclosure, dissemination, other providing behaviours, adaptation or change, and other processing behaviours cannot directly play the role of personal information at a specific time, way, occasion and purpose but can provide conditions for the direct play of personal information, so they do not constitute the use of personal information.

Third, which of these possible uses of personal data can be considered illegal? The illegal use of personal information refers to directly exerting the effects of personal information beyond a reasonable purpose, scope, extent, and manner. It involves the use of personal data in a way that violates the data protection rules. The illegal use of personal information usually takes three objective forms: unauthorized use, false use, and forgery and alteration (Lu and Zhang 2023). Notably, these three forms of illegal use correspond to Prosser's summarization of privacy intrusion (Prosser 1960). Prosser lists four kinds of privacy intrusion: intrusion upon another's seclusion or into another's private affairs, public disclosure of another's embarrassing private facts, publicity that represents another in a false light, and appropriation of another's name or likeness for one's own

advantage. The first type of intrusion is pure intrusion, not the direct use of privacy. The latter three kinds of intrusion are not simple intrusions but further use privacy, and they correspond to and thus help us understand the features of the three forms of the illegal use of personal data. The public disclosure to embarrass is an unauthorized use; the false use of personal data can place others in a false light in the public eye, as can the publicity of others' privacy, and the appropriation of others' names or likeness, although not necessarily in the form of forgery and alteration, is usually for one's own advantage, as is forgery and the alteration of others' personal data.

The first type of behaviour is the false use of others' personal data, which refers to violating the autonomy of using personal data and engaging in activities in the name of the data subject. At this time, the identity data of others are used mainly to attribute the effect of the activity to the data subject. Such identity data theft may cause others to suffer the consequences of failure or illegal activities (Ribet 2023). Examples are using others' identity data to register a company so that others bear the risk of business failure and misusing other people's data for false tax returns, illegal marketing or telecommunications network fraud activities so that the data subject or third party bears the risk of illegal and criminal behaviour. Another behavioural effect of identity data theft is to directly infringe on the interests of the data subject, such as fraudulently using other people's identity data to vote or apply.

The second type is the unauthorized use of others' personal data in activities undertaken in one's name. For example, other people's data can be used for a variety of purposes, such as personalized display, marketing, illegal automated decision-making, and personal portraits. At this time, the effect of the activity belongs to the actors, but they arbitrarily use others' personal data to produce the desired effect.

The third type of behaviour involves falsifying or transforming other people's personal data into data in other scenarios. An example is when the biometric data of others are spliced and transferred to obscene videos or spliced and transferred to records of indecent or illegal events such as prostitution or drug use. At this time, actors are still using others' personal data without authorization, but they have forged or altered others' personal data to produce the desired results.

These three types of behaviour make the illegal use of personal data typed and clear, more in line with the principle of nullum crimen sine lege, to meet the predictability needs of citizens. As Article 3 of the Chinese Criminal Law stipulates, "If an act is expressly prescribed as a crime by the law, it shall be convicted and sentenced by the law; if the law does not expressly provide that the act is a crime, it shall not be convicted and sentenced." Under the basic principle, the legal nature of crime and the clarity of its constituent elements are inseparable (Liu 2010; Xiao 2012). The criminalisation of the illegal use of personal data should determine clear behaviour types of criminalisation, which is a technical requirement of criminal legislation based on the first principle of criminal law (nullum crimen sine lege).

**Criminalisation context**. The illegal use of personal data does not necessarily entail the use of personal data for criminal law purposes. For example, the use of personal data for longer than necessary (establishing the duration of use is a traditional data protection requirement or condition) is not necessarily a use that qualifies as criminal for criminal law purposes. Violating the rules of data protection processing does not itself constitute a crime.

Violating the rules of data use is necessarily a tort. This tort harms the use autonomy of the data subject (the ability to independently decide under what circumstances to use their personal information for what purpose, way and degree) and probably other legal interests. This article explains how examining violations of use autonomy helps explain the application of criminal law. Again, using personal data longer than required may violate privacy and harm the individual; however, does it justify the application of criminal law? There needs to be a distinction between torts and criminal law: something can be criminalised and not dealt with as a tort, and the reverse can also be true. Therefore, the relevance of discussing torts needs to be explained.

For the use of personal data to be criminalised, it first needs to be a tort, violating civil law and data protection rules. Only violations of civil law and data law can qualify as criminal behaviour. A behaviour that is legal according to civil law and data law cannot be criminal behaviour. Civil law and data law are preexisting laws of criminal law, and criminal law safeguards the enforcement of preexisting laws such as civil law and data law (Sun 2012; Wang 2015). Therefore, if there is no behaviour violating preexisting laws such as civil law and data law, criminal law does not need to intervene. In contrast, examining violations of civil law and data protection rules can preliminarily justify the use of criminal law (see the "legal order" in Part 4).

However, even if doctrinally, there is behaviour violating preexisting laws such as civil law and data law, criminal law is not necessarily applied. The intervention of criminal law as a last resort needs rationales other than that the behaviour infringes on a new theoretically recognizable interest that can be and has been recognized in preexisting legal order or that the new interest involves other interests traditionally recognized by criminal law (see Part 4). The additional rationales come mainly from criminal policy (Ma 2007), which can be analysed from the mature framework (see Part 5) in the Model Penal Code developed by the American Law Institute. The code has been translated and advocated by Chinese scholars (American Law Institute 2005). The rationales also concern the legislative technical feasibility (Zhao 2017) of prescribing illegal uses' respective illegality extent, exceptional justifications for using personal data in criminal law and proportionate penalty ranges (see Part 6). These rationales (and limitations) of criminalisation as a context can be used to evaluate the effectiveness of a jurisdiction's approach.

## Investigating the criminalisation of illegal use of personal data

Different jurisdictions have adopted different modes to address the criminalisation of the illegal use of personal information, which suggests that this issue cannot be generalized and needs to be discussed based on the principle of criminalisation while considering the relevant situation of the legal system of personal data protection in specific jurisdictions.

All countries seem to have partially 'criminalised' the illegal use of personal information (and a general principle governing the use of personal information, although not necessarily in a criminal sense). In the case of the Chinese legal system and criminal law, only criminal law can prescribe offences; other laws can prescribe civil torts only such as the Civil Code does or administrative violations such as the PIPL does. Therefore, criminalisation refers to behaviour as a criminal offence with penal treatment in criminal law rather than treating the behaviour with civil compensation or administrative punishments.

**No direct criminalisation**. The first model does not directly criminalise the illegal use of personal data. China's criminal law (Article 253) was amended in 2015 to stipulate the crime of "infringing on citizens' personal information", and it seems that all or at least most of the types of acts infringing on citizens'

personal information can be covered by this crime. However, this crime covers only the illegal acquisition, illegal sale, and provision of personal information and does not address other violations of personal information, such as illegal use. Compared with the relatively complete provisions on the rights of individuals in the processing of personal information in the PIPL issued in 2021, criminal law has not expanded the scope of the crime of infringing on citizens' personal information.

It is difficult to obtain appropriate responses to existing criminal law norms. In the face of the possible criminalisation demand for the illegal use of personal information in criminal policy, the first issue to examine is whether judicial practice can be effective by adequate criminal law interpretation based on existing criminal law norms. Scholars have proposed that the illegal use of personal information after illegal acquisition can be punished under the provisions of Article 253, paragraph 3, of the Criminal Law on the illegal acquisition of personal information (Liu and Song 2022). At this stage, it is not possible to directly crack down on the illegal use of personal information; rather, we can address only on the illegal acquisition of upstream behaviour and then regard this behaviour as a serious circumstance.

However, this line of thinking cannot combat the illegal use of legally obtained personal information. To this end, some scholars have proposed expanding the interpretation of illegal access: the illegal use and processing of facial recognition information can be included in the category of 'illegal' access under the crime of infringing on citizens' personal information (Li 2022). In this case, even if the method of acquisition appears to be legal, it can still be considered illegal as long as it serves the purpose of illegal use at the time of acquisition. However, this interpretation faces the problem of how to prove an illegal use purpose when the actor obtains the information; it cannot address the situation in which there is no illegal use purpose when the actor obtains it or when the illegal use purpose occurs after the acquisition. The use of personal information to commit crimes can be addressed according to the crime committed. However, this approach can address only crimes that have been verified after the fact, such as dissemination after the use of other people's facial information for obscene video synthesis, but synthesis cannot be prevented in advance. Moreover, cases in which personal information is used only to carry out illegal rather than criminal activities, no matter how serious the other circumstances are, cannot be treated as crimes.

The illegal use of citizens' personal information is independent and cannot be included in the current crime of infringing on citizens' personal information through interpretation. Moreover, owing to the different protectable interests of the law, the illegal use of citizens' personal information cannot be covered by other crimes in criminal law. Therefore, although from a practical point of view, there are two ways to criminalise the illegal use of citizens' personal information (judicial interpretation and criminal law amendment), from a reasonable point of view, to maintain the principle of nulla poena sine lege, it is more appropriate to criminalise the illegal use of citizens' personal information through criminal law amendment (Liu 2019).

In this context, Chinese scholars have repeatedly proposed criminalising the illegal use of personal information (Liu 2019); however, whether this proposal should be implemented in the future amendment of criminal law, as well as the specific implementation plan, still needs to be fully discussed by comparing law and theory.

Let us first consider the UK. The UK, as a GDPR-related jurisdiction, adopts the same model of no direct criminalisation of illegal use of personal data as current China does, so it may be insightful to examine how and why it does so. The UK's Data Protection Act 2018 harmonizes a set of principles for data protection and a set of rights for data subjects; however, among the crimes concerning personal data, only illegal acquisition and distribution, such as the processing of personal data (Article 170), reidentification of deidentified personal data (articles 171–172), and alteration of personal data to prevent disclosure to the data subject (article 173), are covered. The reasonable range of criminalisation of infringement of personal data could be considered comprehensively when the rights of personal data and the corresponding crimes of infringing on personal data rights are stipulated at the same time. However, although the United Kingdom has provided comprehensive personal data rights, it has provided only partial criminal law protection for these rights, especially since the illegal use of personal data has not been criminally punished. It seems that British lawmakers believe that the illegal use of personal data is not necessarily criminalised, but the specific reasons for this policy are still unknown.

The unlawful acquisition and publication offences under Section 170 above are old offences inherited from Section 55 of the Personal Data Protection Act 1998, whereas the offences under Sections 171 and 173 are new offences under the Data Protection Act 2018. These two types of new crimes are not stipulated in China's criminal law, which shows that the scope of personal data protection in British criminal law is broader than that in China. The problem, however, is that the illegal use of personal data is still not covered by UK criminal law, in contrast to the crackdown on the two types of acts provided in Articles 171 and 173. This neglect of other acts such as illegal use of personal data seems to be 'arbitrary', and the legislation does not present a consistent rationale for distinguishing between 'do criminalise' and 'do not criminalise'. The explanatory note to the Data Protection Act of 2018 mentions that the act replicates many criminal offences in the 1998 Act and has been amended in line with changes to the legal framework by the GDPR, introducing a small number of new offences to address emerging threats.[3] For example, the Section 171 offence responds to concerns about the security of deidentified data in online files. The UK's National Guardian for Health and Care Data, in its Data Security, Consent and Opt-out Review, called on the government to introduce stricter sanctions to protect unidentified patient data. With the development of big data-driven biomedical research, there are increasing calls for criminal sanctions against the illegal reidentification of anonymized data (Phillips et al. 2017). The integration of law and information technology constitutes the guarantee of criminal law to deter attempts to revert to technologically deidentified personal data (Lin 2019).

However, the illegal use of personal data did not receive sufficient attention in the UK legislation; if the reason is simply that no one raised the threat of the illegal use of personal data during the legislation process, then did anything change between 2018 and the present? Unfortunately, no useful material has been found. However, this finding reminds us that there may be no strong policy reasons to specify the illegal use of personal data in the UK as an offence. Alternatively, from the perspective of legal techniques, some serious cases of the illegal use of personal data can be addressed by other existing offences, such as conspiracies to defraud or unauthorized access to computer systems. However, these reactions are ad hoc and piecemeal rather than coherent in capturing the breadth of illegal use activities or their extent of harm.

In summary, the current mode of treating the illegal use of personal information in China and the United Kingdom is a nonpenal governance mode that involves only civil compensation and administrative punishment. However, it is still necessary to discuss the criminalisation of the illegal use of personal information. Although the GDPR does not harmonize criminal

offences of illegal processing of personal data in Europe, relevant jurisdictions such as the UK and Germany (see 'overall criminalisation' below) have endeavoured to do so but in different models. The reasons for a given jurisdiction's model are not obvious because of either the lack of relevant materials or the lack of rationality of the model itself. However, for China, we have enough information to choose a model, and we can rationally analyse the criminalisation issue being debated. The analysis process and the results can be valuable contributions to a topic that is often difficult to discuss.

In a 2020 official note on the draft of the Personal Information Protection Law, China stated that the 'illegal collection and use of personal information not only harm the vital interests of the people but also endanger the security of transactions, disrupt market competition, and disrupt the order of cyberspace. Therefore, special laws should be formulated and promulgated to regulate personal information processing activities with strict systems, strict standards, and strict responsibilities and implement the legal obligations and responsibilities of personal information processors such as enterprises and organizations to maintain a sound environment in cyberspace.' Here, the illegal collection of personal information and the illegal use of personal information are juxtaposed, but current criminal law makes a clear distinction between them. According to current criminal law, only when illegally used information is illegally obtained does it qualify as a crime of infringing on citizens' personal information and is subject to punishment of the type of behaviour of illegally obtaining personal information towards collaterally cracking down on subsequent illegal use. In 2017, the Supreme People's Court and the Supreme People's Procuratorate interpreted the 2015 amended Article 253 of criminal law and stipulated in Article 6 of the Interpretation of Several Issues concerning the Application of Law to Criminal Cases involving infringement of Citizens' Personal Information that illegal purchase and acceptance of ordinary personal information for lawful business activities, under one of the following circumstances, shall be identified as 'serious circumstances' stipulated in Article 253 of the Criminal Law: Making a profit of more than 50,000 yuan by using citizens' personal information that was illegally purchased or obtained. If the illegal use of illegally obtained personal information fails to meet the above profit standard, the provision of criminal law on illegal access to personal information should not be applied. Moreover, when illegally used personal information is obtained legally, it is more difficult to apply provisions for the crime of infringing on citizens' personal information to regulate the illegal use of personal information.

**Selective criminalisation**. The second model selectively criminalises the illegal use of personal information. The legislation of some jurisdictions, such as the Hong Kong Special Administrative Region of China, supports the criminalisation of the illegal use of citizens' personal information (Liu 2019), but there are differences in the criminalisation conditions. The first condition is the violation of the notification or request of the competent authority for the protection of personal data concerning the reasonable use of personal information. Section 50 of the Hong Kong Personal Data (Privacy) Ordinance applies to an enforcement notice: if, after completing an investigation, the Commissioner believes that the data user concerned is or has contravened a requirement under this Ordinance, the Commissioner may serve a written notice on the data user directing the data user to rectify the contravention and, if appropriate, to prevent the recurrence of the contravention. Section 50A applies to an offence related to an enforcement notice: a data user who does not comply with an enforcement notice commits an offence. On first conviction, he is liable to a fine at level 5 and to imprisonment for 2 years.

Similarly, Japan has stipulated legality requirements for data use, adopting the approach of charging the crime of refusing to comply with the data use security management obligation and criminalising the user if he refuses to comply with the security management obligation notified by the data protection authority. Article 19 of the Personal Information Protection Act amended in 2023 prohibits the improper use of personal information: Companies that process personal information must not use personal information in a way that incites or induces illegal or improper conduct. For example, providing personal information to another company suspected of engaging in illegal conduct, even if there is only the possibility of promoting illegal or improper conduct, is prohibited. Article 148 states the following: (1) if the Committee for the protection of personal information considers that an enterprise processing personal information has violated the provisions and needs to protect the rights and interests of individuals, it may recommend that the enterprise processing personal information or other related information stop illegal acts or take other necessary corrective measures; (2) if an enterprise that processes personal information or other related information receives the recommendations in the preceding paragraph and fails to take measures in accordance with the recommendations without justifiable reasons, the Committee may order the enterprise that processes personal information or other related information to take measures in accordance with the recommendations if it considers that the rights and interests of the individual will be seriously infringed upon; (3) if the Commission considers that an enterprise that processes personal information has violated the provisions of this article, it has seriously harmed the rights and interests of an individual and needs to take urgent measures, it may order the enterprise that processes personal information or other related information to stop illegal acts or take other necessary corrective measures. Article 178 provides for criminal responsibility: a person who violates an order in item (2) or (3) of Article 148 shall be sentenced to imprisonment of up to one year or a fine of up to 1 million yen.

The second type of criminalisation condition criminalises the illegal use of personal information by special groups in business, given their responsibility to protect personal information. For example, Article 179 of the Japanese Personal Information Protection Act states, "An enterprise with personal information, its employees or former employees who, for their own or a third party's illegal interests, provide or misappropriate the personal information database or equivalent that they process in the course of business (including the personal information database or equivalent that has been copied or processed in whole or in part) shall be sentenced to imprisonment of not more than one year or a fine of not more than 500,000 yen." Article 180 stipulates that anyone who provides or misappropriates personal information obtained by an administrative organ in the course of his or her career to seek illegal benefits for himself or herself or a third party shall be sentenced to imprisonment of up to one year or a fine of up to 500,000 yen.

However, the first type of limitation of the scope of criminalisation may require relevant actors to comply with the notice and thus avoid a criminal penalty, but there are other scenarios in which even the first-time violation is serious enough to be criminalised (see the illegality extent issue in Part 6). For the second type of limitation, special groups of actors do bear more duty to protect personal data, but other groups may also seriously infringe upon others (see the black industry chain in Part 5 and the illegality extent in Part 6). Therefore, these two types of criminalisation conditions should be valued, but they are inadequate from the perspective of legal techniques.

**Overall criminalisation**. The third type of criminalisation is that in which the illegal use of personal information is generally criminalised. For example, in addition to the crime of damaging reputation and credit and the crime of divulging secrets, to avoid incomprehensively protecting legal interests, the Personal Data Protection Act of Taiwan, China, also cites criminal means to compensate for the shortcomings of formal criminal law (Lu 2010). This act provides personal data comprehensive protection, which allows it to keep pace with technological developments. For example, in the criminalisation of deepfakes, the existing law already has provisions such as the crime of defamation and the protection act of personal data (Chen 2023). Article 41 of the Personal Data Protection Act of the Taiwan area of China states that in violation of either Article 6 (1) (no collection, processing or use of data relating to the medical records, health, genetic, sexual, medical and criminal records of natural persons, except in the exceptional circumstances listed), Article 15 (no collection or processing of other personal data by the government, Article 16 (governments shall not use other personal data except in the exceptional circumstances listed), Article 19 (nongovernmental organizations shall not collect or process other personal data except in the exceptional circumstances listed), or Article 20 (nongovernmental organizations shall not use other personal data except in the exceptional circumstances listed), causing damage to others; the actor shall be sentenced to fixed-term imprisonment of no more than five years and may be fined not more than NT $1 million.

Here, Taiwan prohibits the illegal use of special and other data by the government and nongovernmental organizations, thus cracking down on the illegal use of personal data in general. If the perpetrator violates the relevant provisions of the law without intent to act in the unlawful interests of himself or a third party or to harm the interests of others, it is sufficient to address civil damage and administrative penalties because of the low degree of culpability. Only when the perpetrator intends to violate the personal information law in the unlawful interests of himself or a third party or to harm the interests of others is the degree of blame high, in which situation a criminal penalty should be imposed. Considering the above intentions, Taiwan's authoritative judicial ruling held that profit is limited to property interests, but damage to the interests of others is not limited to property interests and can include abstract personality interests[4](Xue 2021). The interpretation of the profit from the illegal use of personal data can differ across jurisdictions. For historical reasons, e.g., East Germany Stasi, continental European countries are more alert to surveillance (Igo 2018, pp. 58–59).[5]Germany has generally criminalised unauthorized processing of personal data that are not publicly available. This approach is coherent in addressing all kinds of processing methods for personal data in the same act. Article 42 (2) of the German Federal Data Protection Act 2017 provides for the unauthorized processing of personal data that are not publicly available, in exchange for payment or to profit oneself or others or harm others, with a penalty of up to two years in prison or a fine. Profit here is not limited to illegal interests but also includes the pursuit of legitimate interests, as long as there is no legitimate reason for the use of personal data, such as valid consent, which may limit the rampant use of internet browsing records (Liu 2022).

In summary, the choice and degree of criminalisation of the illegal use of personal information differ across jurisdictions. We need to consider whether China's criminal law regulation of illegal use of personal information, if truly necessary and legitimate, must refer to the second model, represented by Hong Kong and Japan, of limiting the scope of criminalisation and moderating punishment after criminalisation or referring to the third model, represented by Taiwan and Germany, of overall criminalisation. For the second model, we should consider whether the way to limit the scope of criminalisation (see the 'illegality extent' issue in Part 6) is to set conditions such as 'refusing to implement the notice of lawful use of personal information' and 'illegal use of personal information obtained by special groups in business' or whether we should screen the types of behaviours worthy of criminalisation based on the potential harm of the types of behaviours of illegal use of personal information (Kröger et al. 2021; Privacy International 2018). For the third model, we still need to consider, from the perspective of legal techniques, whether there are exceptional legal reasons for using personal information and whether illegal use should be incorporated into the general term of 'unlawful processing' (Shutova 2022) or be listed separately. Specific comparisons and lessons between jurisdictions are further drawn in the following relevant parts. It is unlikely that the options and solutions of a particular jurisdiction would be suitable for any other jurisdiction, so we need to make a specific judgement based on the data theory and the legal system of civil law, data law and criminal law (Part 4) and the basis of legal policies of the personal data protection of a particular jurisdiction formed from the criminal situations of illegal use of personal data and other conduct (Part 5). Finally, we need to address the technical issues concerning criminalising the illegal use of personal data (Part 6).

## Doctrinal legitimacy of the criminalisation of the illegal use of personal data

The illegal use of personal information causes nonnegligible harm in criminal law, which is an essential condition for criminalising the act. According to the theory of fair labelling, if an act commits unique harm, then the harm should be fully reflected in criminal law; otherwise, the characteristics of the act and the damage suffered by the victim are not fully reflected, which does not fulfil criminal justice (Chalmers and Fiona 2008). China should value this perspective of victimology and consider victims' worth and need for protection as important factors in determining the worthiness and need for the penal treatment of an act (Hillenkamp 2018). Therefore, if the illegal use of personal information involves a unique infringement of legal interests compared with the existing offences of illegal acquisition and the illegal provision of personal information, this harm should be fully reflected in criminal law. This part concerns the outlying harms, particularly arising from big data and artificial intelligence (AI). There is a strong focus on use autonomy, but today, this issue also concerns the infringement of other legal interests, such as discrimination.

**Independent protection of the use autonomy of personal data in data theory**. The relationship between privacy protection and personal data protection is a legal issue that has a significant effect on civil rights and social development. To address this issue, scholars have proposed different views based on different legal cultures and social policies (De Hert and Gutwirth 2009; Gellert and Gutwirth 2013; Lynskey 2015, p. 90). Owing to length and subject matter, this article does not debate which position is correct on a macro level. This article proposes that the data theory that conforms to the current legal system of a jurisdiction is the desirable position of that jurisdiction. Both civil law and criminal law in China confused privacy and personal information protection in the early stage, leading to the continuation of the privacy protection mode of the personal information crime clause, which focused on information transfer but failed to examine criminal law needs for personal information protection from the perspective of the full life cycle of the processing of personal information.

Article 2 of the Tort Liability Law enacted in 2009 explicitly stipulates the right to privacy, which is protected by civil law as a civil right. Since then, civil law has explicitly recognized the right to privacy, and Chinese judicial organs have begun to protect this right on a large scale and to try to use it to protect personal information. Article 12 of the Provisions on Several Issues concerning the Application of Law to Civil Disputes Involving Infringement of Personal Rights and Interests through Information Networks issued by the Supreme People's Court in 2014 stipulates: 'Where network users or network service providers use the internet to disclose personal privacy and other personal information of natural persons, such as genetic information, medical records, health examination data, criminal records, home addresses, private activities, etc., causing damage to others, and the infringed party requests it to bear tort liability, the people's court shall support it.' According to this statement, personal privacy is personal information, and there is no substantive difference between the two. However, because the Tort Liability Law only explicitly stipulates the right to privacy, the infringement of other personal information is entitled to the relief rules of privacy. Importantly, the applicable privacy relief rules at this time are designed with respect to the situation of information disclosure, so the relief of personal information is also based on the premise of information disclosure. Article 1 of the 2012 Decision (a single piece of statutory law) of the Standing Committee of the National People's Congress on Strengthening the Protection of Online Information stipulates that 'the state protects electronic information that can identify citizens' identities and involve citizens' privacy. No organization or individual may steal or otherwise illegally obtain the personal electronic information of citizens, sell or illegally provide the personal electronic information of citizens to others.' There is still a gap between the concept of 'citizens' personal electronic information' used here and the concept of citizens' personal information. Although it is divided into electronic information that can identify a citizen's personal identity and electronic information that involves a citizen's privacy, judicial authorities generally consider both of them to be information worthy of protection without substantial differences and often hold that, according to this decision, the protection of both is limited to the scenarios of illegal acquisition and illegal disclosure; that is, both focus only on whether the information is transferred (Guo 2024).

Similarly, Chinese criminal law has taken the position of protecting personal information through information transfer. Since 1979, criminal law has protected some core privacy issues in terms of the crimes of trespassing, illegal search, and the divulging of communication secrets, but its stance is based on whether privacy is illegally obtained. Owing to this logic, the protection of personal information in criminal law adopts the perspective of whether personal information is illegally obtained or illegally sold. In 2009, the Seventh Amendment to the Criminal Law added the crime of selling and illegally providing citizens' personal information and the crime of illegally obtaining citizens' personal information, making it illegal for employees of state organs or financial, telecommunications, transportation, education, medical and other institutions to violate state regulations by transferring citizens' personal information obtained in the course of performing their duties or providing services. The act of selling or illegally providing to others, when circumstances are serious, should be regulated. The reason is that 'some state organs, telecommunications, financial and other units in the performance of official duties or the provision of services to obtain citizens' personal information are illegally leaked from time to time, posing a serious threat to citizens' personal, property security and personal privacy' (Gao 2012, p. 477). At this time, the protection of personal information in criminal law adopts the protection mode of privacy, which is limited to whether the information is transferred from the right holder to the third party. In 2015, the Criminal Law Amendment (IX) expanded the scope of criminal subjects to include any person or unit that violates state regulations by obtaining, selling, or providing citizens' personal information. Cases where the circumstances are serious and involve the commission of a crime and, in the course of performing duties or providing services to supply or sell citizens' personal information to others, face heavier punishments. Accordingly, the charges are integrated into the crime of infringing on citizens' personal information. Currently, the protection stance, which concerns only whether personal information is transferred, continues to hold.

Although it is essentially reasonable for privacy protection to focus only on whether the information is transferred from the perspective of contemporary jurisprudence, this focus is unreasonable for personal information protection. The right to privacy is closely related to human dignity and is primarily a right of passive defence that can be claimed when violated by others, whereas personal information is a more active right that can be actively controlled and used by both the right holder and others according to established rules (Zhou 2018). Traditionally, privacy infringement is an intrusion. The main infringement methods of private activities, private space, and private information are entering, shooting, snooping, eavesdropping, and making information public. As long as private activity information, private space information, and private information are illegally obtained (the information does not even need to be illegally disclosed), a direct violation of the basic dignity of the right subject as a natural person has occurred. Therefore, Article 1032 of the Civil Code stipulates that the content of privacy can be addressed only if the privacy subject explicitly consents or if the law passed by the National People's Congress and its standing committee otherwise allows.

Personal information must be used; if is not allowed, it loses value (Lynskey 2015, pp. 47–50; Guo 2024). The protection of personal information is based on personal information self-determination. Individuals have reasonable control over the entire life cycle of their personal information. With respect to openness and sharing, the ownership and control of personal information in the information network era have been normally separated. This separation is often legal; that is, based on individual sharing, transfer, authorization, or legal provisions, others can legally control the information, but the information subject still enjoys legal protection. In terms of processing stages other than disclosure and sharing, the use of personal information is becoming increasingly technically feasible and economically beneficial in the era of big data (Hilbert 2016; Loideain 2019). In that case, it is necessary to control or safeguard 'on what data is shared, whom it is shared with, or for what purposes data is used or reused'. The value of this type of use possesses characteristics not of personality or exclusiveness, such as privacy, but rather of multiparty sharing and exchange. The right regarding personal information is not limited to passively preventing others from obtaining and disclosing one's personal information but also includes the ability to independently decide under what circumstances others can obtain and disclose one's personal information in what purpose, way, and degree and to independently decide under what circumstances to use one's personal information in what purpose, way and degree (use autonomy). The transfer power to decide that others can obtain and disclose personal information is the preliminary power, whereas the use power to decide that others can use personal information is the core power, which determines the motivation and direction of the exercise of the transfer power (Li 2019). In the era of the development of the digital economy and artificial intelligence, the

status of the right to use is increasingly important in the full life cycle of the autonomous operation of personal information.

**Independent protection of the use autonomy of personal data in the legal order**. The unified regulation of the illegal use of personal information by criminal law can contribute to the expression function of coherent rules in the whole legal order of civil law, data law and criminal law. In principle, criminal law as a last resort serves as a guarantee of the preceding civil and administrative laws (Sun 2012), such as the Chinese Civil Code and the Personal Information Protection Law. If the mode of personal information protection in the preceding law has changed significantly, then the mode of personal information protection in criminal law should also change accordingly to achieve the coherent purpose of an overall legal order. Otherwise, not only can we not effectively regulate personal information infringement behaviour, but we may also damage the overall legal structure of personal information protection.

From the perspective of the overall legal structure of personal information protection, criminal law should be updated according to the preceding laws. The preceding laws of criminal law have begun to cultivate systematic security thinking for the acquisition, storage, and use of personal information. In China's criminal legal system, the protection of personal information should not be limited to the mode of privacy protection that focuses on information transfer. The scope and intensity of protection of personal information should also be explored from the perspective of the whole cycle of personal information processing. The General Provisions of the Civil Law enacted in 2017 refer to the right to privacy and personal information in Articles 110 and 111, respectively, which conceptually indicates to the judicial authorities that the two, although closely related, have different rights and interests. However, the law does not clearly define the contents of the two, which makes it possible for judicial organs to still use the right to privacy to protect personal information or personal information to protect privacy in practice. Fortunately, Article 76 of the Cybersecurity Law enacted in 2016 stipulates that personal information refers to all kinds of information recorded electronically or in other ways that can identify a natural person's identity alone or in combination with other information, including but not limited to the natural person's name, date of birth, ID number, personal biometric information, address, and telephone number. This article explicitly states that the judicial authorities shall apply the provisions of personal information to protect the case by the definition of personal information; only in cases that do not meet the definition of personal information can we consider applying the terms of privacy protection. This statement establishes the dual protection of privacy and personal information at both the legislative and judicial levels. In addition, the Civil Code enacted in 2020 systematically provides 'protection of privacy and personal information' in Chapter VI. Article 1032 defines privacy as follows: 'Privacy is the private space, private activities, and private information that a natural person has in his or her private life and is unwilling to be known to others.' Article 4 of the Personal Information Protection Act 2021 defines the definition and type of processing of personal information as follows: 'Personal information is information recorded electronically or by other means relating to an identified or identifiable natural person, excluding information that has been anonymized. The processing of personal information includes the collection, storage, use, processing, transmission, provision, disclosure and deletion of personal information.' These provisions clarify once again that the protection of privacy and personal information should, in principle, be binary and parallel. Personal information should have its own independent and complete protection mode.

From the perspective of effectively regulating personal information infringement behaviour, criminal law should be updated according to the preceding laws. Current criminal law focuses only on the illegal acquisition, sale, and transfer of personal information, adopting a piecemeal, ad hoc, and reactive approach that currently fails to match the scope and extent of the illegal infringement of personal information. A lack of agreement concerning the definition and liability of the illegal use of personal information makes it difficult to enforce legal compliance, and most information users choose to create their form of best practice rather than follow explicit industry advice. Therefore, we should fully express society's condemnation of illegal phenomena and its demand for justice, redress, and change through a coherent legal response (McGlynn and Rackley 2017). Like behaviour in general, law has an expressive function (Sunstein 1996). This function can be used to promote cultural change. Law conveys, affirms, solidifies, and restores existing social norms, commitments, and beliefs while clarifying new ones and plays a key role in protecting our rights to be treated as members of society with a good and civilized capacity (Waldron 2012; McGlynn and Rackley 2017). This combination of identification and formation has played a key role in addressing the issue of information technology-based personal information infringement (illegal use), enabling the law to be enforced. A coherent, and therefore clear, widely known and understood framework of criminal law provisions and judicial interpretation can create an important cultural climate of respect for personal information and trust in legal protection in the information technology environment to prevent the approval and establishment of an industry and culture that uses information technology solely as an object of exploitation.

**Independent protection of the use autonomy of personal data for substantive interests**. From the perspective of criminal law doctrine, whether an act should be considered criminal depends first on the threat of infringement to the interests protected by criminal law and requires comprehensive consideration of the possibility of harm (Feinberg 1984, p.216) and the urgency of such harm (Guo 2023). The urgency of harm affects the ability of the victim and the public authority to intervene in time to reduce and eliminate the possibility of harm. The illegal use of personal information is more urgent than the unlawful acquisition and provision of personal information. The act of illegally obtaining and providing personal information obviously infringes only on the right to transfer personal information in an abstract sense and cannot directly infringe on the substantive rights and interests of the information subject, such as personal safety and property safety, and the substantive harm to the information subject is still far removed. A hacker can obtain bank details, but the money is still in the account. Illegal uses of personal information, such as creating personal portraits, further telecommunications network marketing, and travel tracking, cause direct harm to the substantive rights and interests of the personal information subject. For example, harassing marketing will directly infringe on the peace of the personal information subject; discriminating against familiar guests based on the big data of customers and the personal data of familiar guests will directly infringe on the right to fair trade; and precise fraud via personal information will directly infringe on the property of the personal information subject and even lead to suicide, self-harm, and other personal harm consequences.

Criminal law does not consider trivial matters; otherwise, it would violate the principle of proportionality, and ultimately, the

gain is not worth the loss (Baker 2011, Chapter 3). Therefore, all types of infringement of personal information to be combated by criminal law can cause serious harm. The illegal use of personal information is precise in terms of the damage it causes, whereas the unlawful acquisition and provision of personal information tends to be more large scale. Personal information is identifiable, but this characteristic is often reflected only as a possibility under circumstances of illegal acquisition and illegal provision; that is, the actor may identify a large number of victims, but if the actor has no purpose of directly using personal information, the actor often will not take time and effort to convert this possibility into reality. In the case of illegal use, the perpetrator will spend the necessary time and energy to link each piece of personal information to a specific subject and then carry out marketing, identity theft, or telecommunications network fraud and other personal information use activities against the particular subject (Liu and Song 2022). The harm of illegally obtaining and illegally providing personal information is cumulative, i.e., the infringement on the personal information transfer power of a large number of individuals has reached the criminal requirements of serious harm. The illegal use of personal information can easily have a significant effect on the rights and interests of specific individuals; thus, the amount of illegally used personal information likely does not need to be very large to meet the requirements of serious harm required for criminal law intervention.

## Policy necessity of criminalising the illegal use of personal data

Another necessary condition of criminalisation is compliance with criminal policy. From the perspective of criminal policy, behaviour that interferes with use autonomy and other legal interests can be a candidate for criminalisation, but the criminal law system would adopt either a stern or a lenient standing towards conduct according to policy considerations (Ma 2007). These policy considerations can vary and be vague in different jurisdictions, but we can refer to a mature framework. According to the legislative rationale specified in the American Law Institute's Model Penal Code, criminal law should combat harmful conduct that disrupts the sense of security of the community, which either is particularly harmful or is less harmful but more likely to be inflicted on others by those who clearly have no respect for the rights of others.[6] In jurisdictions where information technology such as big data and AI is widely available, such as China, the criminalisation of the illegal use of personal information generally meets both criminal policy grounds. When a tort meets criminal policy grounds, it can be considered criminal law.

**Egregious nature of the illegal use of sensitive personal data.** The illegal use of sensitive personal information is likely to cause particularly serious harm. Sensitive personal information is defined in Article 28 of China's Personal Information Protection Law as 'personal information that, once leaked or illegally used, is likely to lead to the violation of the human dignity of natural persons or harm the personal or property safety, including biometric information, religious beliefs, specific identities, medical and health information, financial accounts, whereabouts, etc., and personal information of minors under 14 years of age.' This definition reveals that the illegal use of sensitive personal information can easily lead to serious harm to human dignity or personal or property safety. If this type of behaviour is one-time and accidental, the nature of its harm generally does not reach the particularly serious degree of murder, arson, rape, or pillage; however, if a certain amount and time limit are superimposed, the overall degree of harm will be particularly serious and should receive attention from criminal law.

In recent years, Chinese scholars have begun to examine the illegal use of special types of personal information. For example, facial information is an example of sensitive biometric information. Technically, a deep fake also involves the use of personal biometric information. The front-end liability thinking of citizens' personal information protection, which focuses on illegal acquisition behaviour, ignores the independence of legal interest in infringing on deepfake behaviour and the special need for personal biometric information protection. It is argued that the normative nature of deepfakes is identity theft, so it is necessary to introduce the concept of identity theft in criminal law to compensate for the gap in criminal law evaluation concerning the 'legal acquisition + illegal use' of personal information (Li 2020). Identity theft causes harm different from, but more serious than, the simple illegal acquisition of personal information (Ribet 2023). Some scholars have proposed that in addition to the general characteristics of personal information, personal financial information has outstanding characteristics, such as a significant economy and considerable credit, because it occurs in financial activities. The illegal use of personal financial information seriously infringes on individuals' privacy and individuals' property rights, promotes many downstream crimes, such as money laundering and telecom fraud, damages the reputation of financial institutions, hinders the development of the financial industry, and has many negative effects on financial stability and the financial environment. At the legislative level, the crime of the illegal use of personal financial information should be added (Li 2019). In this context, the use of some sensitive personal information violates the personal dignity of an individual, a particularly important personal right, because some sensitive personal information involves private information in personal privacy, which requires more legal regulation than does the ordinary infringement of personal information that does not involve private information.

**Worse situation of the large-scale illegal use of ordinary personal data**. Although the illegal use of ordinary personal information is less harmful than the illegal use of sensitive personal information, it is more likely to be imposed on ordinary citizens by criminals who clearly do not respect the personal information of ordinary citizens. Scholars have noted that the illegal use of personal information has become increasingly fierce, driven by excessive profits. The crime of infringing on citizens' personal information has gradually formed a complete data transaction black industrial chain of 'provider - middleman - illegal user', with a clear division of labour and tight organization with respect to each link. That is, personal information is clearly priced, upstream 'middlemen' are responsible for illegally obtaining, selling, and providing personal information, and downstream demand groups buy and use personal information to carry out various illegal and criminal activities. These phenomena include using other people's personal information to maliciously register internet accounts, fraudulently using personal information to apply for credit loans or tax evasion, stealing personal information to hack the identity authentication system, abusing personal information to make harassing false marketing calls, pushing harmful information, and causing illegal debt collection to become increasingly serious (Cao 2019; Liu 2020). The industry model of making profits by illegally using personal information to carry out criminal activities is the root cause of personal information leakage and the proliferation of illegal transactions. The illegal use of personal information is a downstream behaviour, causing great damage to or threats to citizens'

personal and property safety and social management order. Compared with the upstream illegal transfer of personal information, the illegal use of personal information involves more serious infringement of legal interests, which manifests as the root, direct, and precise infringement of legal interests (Liu and Li 2022). In 2023, the Beijing Higher People's Court issued the White Paper on the Trial of Crimes of Infringing Citizens' Personal Information, which noted that crimes infringing on citizens' personal information are frequent and that nearly 40% of these crimes are used for illegal and criminal activities (Lin 2023). In the eyes of the actors involved in the personal information black industry chain, the subject of personal information is only the object of their profit-making illegal and criminal activities, and they do not consider the subject status of the other party. This black industrial chain subculture atmosphere that does not respect the subject status of others' personal information should receive attention and be managed; otherwise, it will be interfere with the need to promote the development of information networking in a country. By definition, criminals cannot care less about their victims' personal data. However, this kind of personal character disrupts the sense of security of the community and should be targeted by criminal law.

An important reason why practitioners in the black industry chain apparently do not respect the autonomy of the use of personal information is that the current criminal justice system does not demonstrate effective crime prevention. The illegal use of personal information is more direct and results in even higher profit than does the unlawful acquisition and provision of personal information, so the temptation to commit this behaviour is greater. On the other hand, although this behaviour is easier to detect than the illegal acquisition and provision of personal information is, it is currently not punishable by criminal law. That is, it is difficult for citizens to discover that their personal information is illegally obtained, sold, and provided, and even if they make this discovery, it is difficult to find the perpetrator by themselves, while it is relatively easy for citizens to find that their personal information has been used. In this case, if the illegal use of personal information is not criminalised, citizens seeking public relief may not be accepted or may be rejected by public authorities (Tian 2023). Because the chain of behaviours of illegally obtaining, selling, and providing personal information is long and complex, it is difficult for victims and judicial organs to identify every specific perpetrator, whereas the nodes of illegal use of personal information are easier to detect, and it is thus easier for victims and judicial organs to identify the particular perpetrators of illegal use. If the easily identified actor is not deterred by a penalty, then the actor who directly uses personal information to make an enormous profit will naturally tend not to respect the autonomy of using personal information. The situation is that, where the commercial benefits of using personal data, for example, through targeted advertising, are substantial, the current milder sanctions against abuse often fail to deter it (Zharova and Vladimir 2017). Illegal use is thus more likely to be inflicted on data subjects, which exacerbates the subculture atmosphere that does not respect others' subject status.

## Technical feasibility of criminalising the illegal use of personal data

For scientific legislation, the criminalisation of the illegal use of personal data should balance the protection of personal data and the interests of relevant parties (Gaagouch 2024). Criminalisation might lead to further legal uncertainties in practice and create additional hurdles for data controllers, processors and collectors, which could hinder the usage of personal data as well as the free flow of such data, ultimately impacting innovation in general. However, a balance can be achieved, and the potential chilling effect of overly strict data protection regimes on the market can be avoided by criminal law techniques of setting high and clear illegality extent requirements for personal data use, requiring diversified and practical justifications for personal data use, and establishing proportionate and clear penalty ranges for the illegal use of personal data.

**Illegality extent of personal data use in criminalisation**. For criminalisation technology, we should be able to determine the extent of the illegality of various personal data use scenarios. Based on the argument of the necessity of criminalisation, we should distinguish the abuse of information from ordinary illegal use and include the abuse of information under the crime of infringing on citizens' personal information (Li 2019; Gon and Li 2022). As summarized in the second part of this article, limiting the scope of criminalisation and differentiating criminalisable abuse of personal data from ordinary illegal use can be a way of setting criminalisation conditions such as ex post 'refusal to perform official notice' or belonging to 'special groups of actors on duty' in the laws of Japan and Hong Kong, but the types of behaviours that qualify as criminal should generally be screened according to the potential harm caused by the specific types of illegal use of personal information. More specifically, it should be determined whether the necessary severity for criminalisation is achieved according to the degree of infringement of the specific behaviour type on the autonomy of using personal information, the degree of harm to other legal interests, and the degree of personal danger to the perpetrator.

First, in terms of the extent of infringement of the freedom to use personal information, the illegal use of others' personal information and the direct infringement of others' major interests seriously infringe on the autonomy to use personal information and should be criminalised. (1) The illegal use of personal information to infringe on the types of interests already protected by criminal law can be used as a clear criminalisation threshold. For example, the 2020 amendment to the Criminal Law added Article 280, titled 'crime of impostor', to protect citizens' admission qualifications for higher education, civil service employment qualifications, and employment placement treatment, which increased the types of interest protected by criminal law. In practice, such cases have occurred. By convincing candidates to enter their details in a 'preregistration system', the perpetrator illegally obtained the information used by candidates to log into the college choice registration system and then, against the wishes of candidates, arbitrarily filled in another application for college A, resulting in a total of 11 students being wrongly admitted to college A.[7] In this case, the degree of infringement on the use autonomy of personal information should be considered to have reached the threshold of crime. (2) The fraudulent use of personal information, unauthorized use of personal information, forgery, and alteration of personal information in other scenarios, if enough to cause the information subject to bear the consequences of crime or enough to prompt the perpetrator to commit criminal acts, should be considered to have reached the threshold of criminalisation. These situations include the misappropriation of other people's information for telecommunications and network fraud, unauthorized use of other people's information for illegal business activities, forgery, alteration of other people's information for the production and dissemination of obscene materials, extortion, and fraud. (3) For the fraudulent use of multiple types of personal information, unauthorized use of multiple types of personal information, forgery, or the alteration of multiple types of personal information in other scenarios, although the interests of each individual are minor, the cumulative degree of infringement

on the use of personal information autonomy is serious, so illegal use should be criminalised. The organizational and systematic use of personal information is the basic form of the illegal use of personal information (Jian 2022). Article 5, paragraph 1, items 3–7 of the Interpretation of Several Issues concerning the Application of Law in Handling Criminal Cases involving Infringement of Citizens' Personal Information by the Supreme People's Court and the Supreme People's Procuratorate stipulate the quantitative conditions for illegally obtaining, providing, and selling multiple types of personal information and infringing on the autonomy of personal information transfer to a serious degree: illegally obtaining, selling or providing 50 or more items of whereabouts and tracking information and communication contents, credit information or property information; illegally obtaining, selling or providing 500 or more items of accommodation information, communication records, health and physiological information, transaction information and other personal information of citizens that may affect the safety of a person and property; illegally obtaining, selling or providing 5000 or more items of citizens' personal information other than those provided for the items above; and illegal gains of 5000 yuan or more. The illegal use of personal information is a violation of personal information use autonomy that is no less serious than the illegal acquisition, provision, and sale of personal information. Therefore, the above criminalisation standards should apply to the illegal use of personal information, especially in the scenario of automated decision-making and personal portraits.

Second, in terms of the infringement of other interests, the illegal use of personal information obtained by special groups relying on business convenience not only infringes on the use autonomy of personal information but also infringes on the trust of users and the public in the legitimacy and security of special businesses and should be criminalised. When an organization or other unit authorized by a state organ, law, or regulation to manage public affairs uses, unlawfully uses, forges, or alters a citizen's personal information obtained in the course of performing its duties or providing services, this behaviour should be criminalised. In addition, concerning the provisions of Article 5, paragraphs 1 and 8 of the above judicial interpretation, the criminal standards for the illegal sale and provision of personal information by special groups are halved, and those who illegally use the personal information of citizens obtained in the process of performing duties or providing services, the amount of which reaches more than half of the criminal standards for the above illegal use of multiple types of personal information, should also be criminalised.

Third, in terms of the degree of personal danger to the perpetrator, for those who refuse to comply with the notice of the lawful use of personal information by the competent authorities and those who have received criminal penalties for violating personal information or have been charged administrative penalties within the last two years and then illegally use personal information, crime prevention is necessary, and their conduct should be criminalised. The model of 'refusing to comply with the notice of lawful use of personal information', which is a violation of administrative obligations, as a prerequisite condition of constituting a crime, on the one hand, comes from the experience of setting the threshold of crime in Hong Kong law; on the other hand, the crime structure is similar to the crime of refusing to comply with the network security management obligation that was added to China's criminal law in 2015. The establishment of the crime requires the network service provider to refuse to correct their behaviour after being ordered to correct it, and the circumstances are serious. The illegal use of personal information violates the autonomy of using personal information. The refusal to comply with the notice further indicates the personal danger of the perpetrator and highlights the direct possibility of subsequent infringement of the autonomy of the use of personal information, so it should be criminalised. Similarly, those who have received criminal punishment for infringing on personal information or have received administrative punishment within the last two years and then illegally use personal information not only have directly infringed on the autonomy to use personal information in this instance but also have demonstrated the direct possibility of further infringing on the autonomy to use personal information through prior punishment and should be criminalised. This example already corresponds to the Chinese experience in personal information protection and other criminal governance.[8] Moreover, the subjective use of personal information to make illegal profits should be criminalised. As mentioned in the third section, Taiwan criminalises the illegal use of personal information to obtain illegal benefits, whereas Germany criminalises the illegal use of personal information to obtain benefits. Compared with other perpetrators, perpetrators who intend to obtain illegal benefits clearly are subject to greater reprehensibility and personal risk. The former reflects the worse subjective intention of the perpetrator, and the behaviour can be treated only as a crime when it causes a high degree of social harm in China. When the behaviour causes only a low degree of social harm, it can lead to administrative punishment. Therefore, in terms of criminal law regulation of the illegal use of personal information, it is more appropriate to take the intention of obtaining illegal benefits as a criminalisation condition.

**Justifications for personal data use**. For the behaviour of using personal data, if an actor has a legal reason to use it, even if its infringement reaches the illegal extent discussed above, this behaviour cannot be criminalised. For defences against the use of personal data, most criminal law scholars adopt the perspective of interest balance; that is, the illegality of the use of personal data is excluded when the interests that can be achieved by using personal data exceed the interests involved in the use of personal data. However, the interest balance approach may have certain defects, and it is difficult to strike the necessary balance between sharing and control. In principle, the more closely related the physical or spiritual aspects of individuals are, the more personal data should be included in the scope of personality rights to be protected and not allowed to be exceeded at will by other interest considerations (Miruć 2013; Tong 2024). The reason for this principle is that personal information can contain private information, and Article 990 of the Civil Code stipulates that the right to privacy belongs to the rights of personality. Article 1034 stipulates that private information in personal information is, in principle, subject to the protection rules of privacy rights, and if there are no applicable rules, provisions on the protection of personal information are applicable. Therefore, we should first clarify the legal reasons for the use of private information in personal information, when the protection rules of privacy are applied, and then explore the legal reasons for the use of other personal information. At this time, we can systematically examine the legal reasons for the use of personal information via the tripartite method (privacy–individual–society) of German 'domain theory' (Wang 2017) and the resulting domain distinction of personal information (Zhang 2001, p. 372; Tong 2024). The following figure, Fig. 1, "domain distinction of personal information", shows the important differences between the intimate, private and social spheres. The delicate differences between the intimate, private and social spheres are discussed in the next paragraph.

The fourth part of this article demonstrated that the subject's control of information transfer under the privacy protection

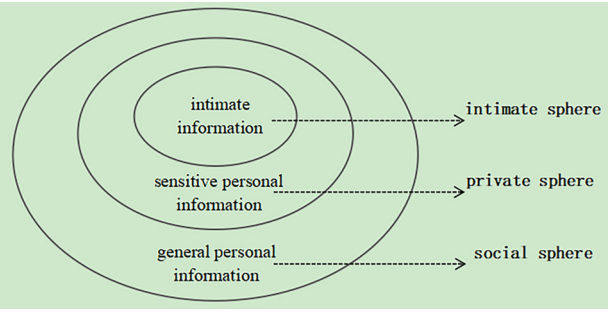


**Fig. 1** Domain distinction diagram of personal information.

mode is not enough to protect the subject's autonomy in personal information use. The derivation and development of personal information are closely related to the protection of privacy by law. However, with changes in the social economy and technological environment, the pattern of information infringement has changed, and the perspective and focus of legal protection have also changed. In the first stage, the law focused on the right to privacy represented by the individual's right to be alone in the intimate sphere and focused on the right not to make the intimate sphere public, mainly against the intrusion of media gossip (Warren and Brandeis 1890). From the perspective of personal information, if private information is identifiable by an individual, it is also personal information and requires strong legal protection. The personal information category in this stage still exists in contemporary society. However, personal information is not limited to this category. In the second stage, with the development of information technology such as computer technology, the privacy of private areas should still be protected, but it is difficult to disclose it under the threat of eavesdropping, stealing, and other devices. At this time, the focus of personal information autonomy began to shift to the private sphere, in which the decision to hide or present inherent personal information related to inner spirit and characteristics was made in interpersonal relationships (Jian 2022). The protected autonomy of information was limited not only to hiding but also to presenting. However, the root cause of both is that once this inherent information is disclosed or used, it can easily harm personal dignity and personal and property safety, and this information often contains sensitive personal information, for example, personal information in the German census case (Igo 2018, pp. 58–59). At this time, less attention was given to the protection of ordinary personal information, as exemplified by the prevalence of telephone directories. In the third stage, in the high information age supported by information technologies such as networks, big data, and artificial intelligence, individuals' personal information, especially nonsensitive information, is routinely and efficiently collected in the daily social sphere. However, such information is edited, reorganized, and subjected to other data analysis in the information system, which can still portray a group or individual image and can still cause damage under different use situations (Igo 2018, p. 164). Therefore, the use of personal information in general should also set appropriate boundaries. The reasons for legalizing the use of personal information in the private, personal, and social spheres are discussed in detail below.

First, private information in personal information involves the right to privacy, and the legal right approach should be applied in this area of privacy, i.e., the reasons for its lawful use should be determined by the protection rules of the law for such rights. Article 1033 of the Civil Code stipulates that the legitimate cause of the infringement of privacy is otherwise provided for in laws passed by the National People's Congress and its Standing Committee or with the explicit consent of the right holder. Currently, there is no legitimate cause based on interest balance that the user of personal information can claim in a specific scenario, so private information such as whereabouts and track information, communication content, credit information, and property information cannot be used in principle. Users are bound by benefits protected by the law. Article 8 of the general provisions of the Civil Code stipulates that civil subjects engaged in civil activities should not violate the law or public order and good customs. Public order and good customs are types of public interest. Therefore, in the case of the consent of the right holder of private information, the user should not violate the interests of public order and good customs by using private information. For example, public figures and families have exercised 'transparency' in the case of political and economic interests, allowing the media and the public to know all aspects of their lives, and politicizing and commercializing personal family reality shows have emerged. The 'confessional culture' has also arisen through the emergence of a variety of individual expressions by the general public, both voluntarily and without obvious public or political intentions (Igo 2018, p. 324).

However, regardless of the purpose for which individuals voluntarily consent, the use of private information is limited by a society's definition of the interests of public order and good. The use of most core private information, such as sexual images, is obviously against public order and good customs. Even if Article 13 (5) of the Personal Information Protection Act stipulates that news reporting in the public interest can process personal information within a reasonable range without the consent of the information subject, users of private information must not violate the public order and good customs. Otherwise, the use cannot be justified in criminal law. For example, in the Japanese Ministry of Foreign Affairs leak case, a journalist asked a Ministry of Foreign Affairs civil servant to provide information about the secret telegraph in the return of Okinawa; otherwise, the journalist threatened to disclose private information about the existence of an illicit relationship between the servant and another individual. The Supreme Court of Japan pointed out in its ruling that the means of the perpetrator were not justified. The use of other people's sexual information to force the public report of the telegraph is against public order and good customs (Maeda 2017, p. 215). However, if a citizen exercises the right of public opinion supervision under Article 41 of the Constitution of the People's Republic of China to complain, accuse, or report, such information may be used for online public opinion supervision if the complaint to the competent authorities fails. However, online reporting and supervision should have a clear right basis and factual basis, and information disclosure of the informant against the target individual should conform to the principle of proportionality (Wang and Huang 2024). In this case, the use can be justified in criminal law.

Second, sensitive personal information is closely related to the personal domain of individual natural persons and directly affects their feelings concerning their important interests. Sensitivity is the natural person's tendency to feel a certain amount of pain and pleasure, and its degree of existence is different (Bentham 1789). This type of difference objectively comes from the degree of damage and danger of specific information to specific important interests of particular subjects in specific scenarios. Therefore, to determine the legality of the use of personal information in the private sphere, the interest balance approach can be adopted. The infringement and danger arising from the use of personal information can be ignored when more important interests can be safeguarded. Based on this 'obvious' standard, the protection of sensitive personal information should be emphasized, and its use should be cautious. Sensitive personal information such as

accommodation information, communication records, health and physical information, financial accounts, and transaction information can easily affect the personal and property safety of the information subject if it is leaked or used. For sensitive personal information such as health information, a code of conduct needs to be adopted to ensure greater transparency and accountability in its use (Staunton 2021). Even if the information has been self-disclosed or if other information has been legally disclosed, if its use is likely to have a significant effect on the rights and interests of individuals, consent should be obtained separately according to the rules for processing sensitive personal information (Articles 27 and 29 of the Personal Information Protection Act). If the use of disclosed sensitive personal information easily affects the personal and property safety of some information subjects but the affected personal and property safety itself is not significant enough, including life and health, major property, or other core interests, the users do not need to obtain separate consent.

However, this conclusion only concerns the legality of the use of disclosed sensitive personal information by the Personal Information Protection Act. A lawful cause under the Personal Information Protection Act is, of course, a lawful cause under the Criminal Law, but an illegal situation under the Personal Information Protection Act is not necessarily an illegal situation under criminal law because the application of criminal law also takes into account the necessity of criminal strikes. From the perspective of comparative law, Article 6, paragraphs 1 and 3 of the Personal Data Protection Act of Taiwan expressly stipulate that data related to a natural person's medical treatment, health care, heredity, sexual life, physical examination, and criminal record can be used if they have been explicitly disclosed or legally disclosed by the data subject (Dove and Chen 2021). The Personal Information Protection Law of China imposes additional restrictions on the use of sensitive personal information that has been explicitly disclosed or legally disclosed by the information subject, which is already a relatively strict provision. On this basis, sensitive personal information that has been explicitly disclosed or legally disclosed by the information subject has reduced the protectability of interests, and it is no longer necessary for China's criminal law to use penalties to crack down on the use of such information. Another consideration for legislators may be that in the era of the digital economy, economic entities need to make the best use of personal information to gain competitive advantages in the competitive environment. This contradiction between survival and compliance with prohibition leads to the unsatisfactory effect of criminal prohibition (Wang 1999).

Third, general personal information belongs to the social sphere and has significant social value in the digital economy and society. To the extent that its use can promote more important interests, such use may be considered legitimate grounds in criminal law. More important benefits can come from national security, public interest, data subjects, other people, government statistics, and academic research. However, two details are noteworthy: (1) Government agencies or academic institutions may use personal information for statistical or academic research for public benefit purposes, provided that such information processed by the information provider or disclosed by the information collector will not lead to the identification of specific information subjects (Articles 16(1)5, 20(1)5 of the Personal Data Protection Act of Taiwan). This requirement serves to anonymise the use of personal information as a security measure. (2) Nongovernmental organizations may be interpreted as using personal information for marketing purposes in the public interest or the interest of the information subject but should stop using personal information for marketing purposes if the information subject objects (Article 20 (2) of the Personal Data Protection Law of Taiwan). At this time, the interests pursued by the nongovernment subject in the use of personal information are judged by the information subject as not superior, and the law should support this judgement in the business scenario of the nongovernment subject. This statement expresses the reason for economic efficiency. A mentally competent, fully informed individual can choose through a process of rational self-reflection based on his preferences, which are formed in his lived experience, and he can better than anyone else identify, weigh, and know what is best for his interests (Gal 2018).

**Penalty range for the illegal use of personal data**. Scholars believe that the crime of infringing on citizens' personal information, in Article 253A of the Criminal Law, can include new types of illegal use of personal information, and it is not necessary to specify a new crime to account for this behaviour. Rather, setting up the illegal use of personal information as a separate subsection within the crime of infringing on citizens' personal information is appropriate. In terms of penalties, considering that the illegal use of personal information is more harmful to the legal interests of personal information autonomy than illegal provision and illegal access are, the legal penalty for the illegal use of personal information should be appropriately greater than that for illegal provision and illegal access (Lu and Zhang 2023; Wen 2023). From the principle of proportionating the crime and the punishment, the more serious the infringement of legal interests the crime causes, the greater the range of legal punishments that should be assigned to ensure criminal justice. However, judging from China's existing legislative practices and comparative law experience, it is not appropriate to set penalties for the illegal use of personal information that are much greater than those for illegal acquisition and illegal provision.

First, in the protection of real information and signs, China's criminal law has adopted the position of setting the same legal penalty range for its acquisition and use. In Article 219 of the Criminal Law, illegal use and improper acquisition and disclosure are listed in the same category, and in Article 375 of the crime of forgery, theft, trading, illegal provision, and illegal use of the special symbol of the armed forces, illegal use is listed in the same category as illegal acquisition and illegal provision. Criminal law does not provide a separate higher legal penalty range for illegal use. The reason may be that the statutory penalty of less than three years of imprisonment for basic offenders and more than three years of imprisonment for aggravated offenders was originally set based on the substantial degree of the legal interest harm of illegal use, and illegal acquisition and illegal provision before illegal use are presumed by lawmakers as causing legal interest infringement equivalent to that caused by illegal use (Guo 2024). The United States Model Criminal Code also adopts the 'substantial steps' standard to distinguish the stages of unpunishable conduct points from those of punishable conduct points (Dubber 2015, pp. 114–116). Thus, the legal penalty range of illegal use applies to illegal acquisition and illegal provision. Therefore, since the legal penalty range of illegally obtaining and illegally providing personal information has reached the prison term of less than three years for basic offenders and more than three years and less than seven years for aggravated offenders, the legislation has already considered the penalty range for subsequent illegal use, and there is no need to further increase the legal penalty range of the illegal use of personal information.

Second, concerning comparative legal experience, most jurisdictions for the illegal use of personal information prescribe a legal penalty lower than the maximum penalty for the crime of violating citizens' personal information in China (seven years of imprisonment): one year in Japan, two years in Germany and

Hong Kong, and five years in Taiwan. Given the background of the heavy penalty structure in China, we should be careful when allocating heavy penalties for new crimes. At the same time, legislative experience in comparative law has shown that in the era of the digital economy, personal information is often used to obtain benefits, but this behaviour often causes damage. Therefore, more research should be conducted on the setting and application of the fine penalty, that is, how to distinguish and match the fine penalty with the freedom penalty, to precisely apply them in specific cases. For example, scholars have studied the application of fines for crimes involving illegally obtaining, selling and providing personal information (Ren 2024).

## Conclusion

Concerning the criminalisation of the illegal use of personal information, investigations of the comparative laws of Britain, Japan, Germany, China's Hong Kong Special Administrative Region, and Taiwan provide a window for self-examination and comparison. In the current era, when internet information technology penetrates nearly all aspects of our lives, the illegal use of personal sensitive information may lead to serious violations of the victim's personal dignity or personal and property safety. Additionally, the illegal use of general personal information as the downstream link in the black industrial chain of data trading is becoming increasingly rampant in the age of AI. Regulation through the intervention of criminal law has sufficient legitimacy in jurisprudence and practice. However, limited by the narrow perspective of 'information transfer' in the campaign of privacy protection, even if all interpretation means within the legality limit are exhausted, China's existing criminal law norms still show a particular weakness in cracking down on the illegal use of personal information. Therefore, expanding the existing crime of infringing on citizens' personal information in the form of amendments may become the appropriate way for criminal law to respond to changes in social life and exercise the functions of prevention and protection.

On the other hand, criminal law is a 'necessary evil' (Chen 2017, p. 25). After all, it should be prudent to draw appropriate boundaries in the criminal regulation of crimes via personal information. This task essentially considers the question of how to strike a balance between protecting citizens' autonomy in using their personal information and fully appreciating the public value of data circulation. Japan and China's Hong Kong Special Administrative Region provide a way to control the scope of crime by setting the conditions of 'refusing to perform official notice' or 'special groups of actors'. On this basis, a comprehensive judgement should be made concerning whether criminal law is worth applying according to the different types of illegal use behaviours, with a focus on the degree of infringement on the use autonomy of personal information under specific scenarios, the degree of harm to other interests such as public trust, and the degree of personal danger represented by the behaviours. In addition, by distinguishing the degree of protection between private information, sensitive personal information, and general personal information, legal reasons that can exclude criminal wrongfulness can be clarified in the corresponding private, personal, and social spheres. Finally, considering the consistent legislative thinking and overall penalty structure of China in comparison with relevant jurisdictions, the legal penalty for the illegal use of personal information should be consistent with the behaviour of providing and obtaining that information.

## Data availability

Data sharing is not applicable to this research as no data were generated or analysed.

Received: 17 October 2024; Accepted: 29 May 2025;
Published online: 09 June 2025

## Notes

1 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and the free movement of such data and repeal of Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.
2 Functionally, personal information and personal data have the same value, and the two terms are often used interchangeably in the legal context in many countries. Therefore, this article does not differentiate between these two terms.
3 Explanatory Notes of Data Protection Act 2018, para 48.
4 Criminal Decision No. 1869 of the Supreme Court of Taiwan.
5 *R(T) v Chief Constable of Greater Manchester*[2015] AC 49 at [88]-[89].
6 Model Penal Code § 250.7 cmt. At 44 (Tentative Draft No. 13, 1961).
7 Case of He Jianheng and Deng Xiyao Destroying Computer Information System. Criminal Judgment No. 188 of Qingxiu District People's Court of Nanning, Guangxi Zhuang Autonomous Region (2019) GUI 0103.
8 The Supreme People's Court and the Supreme People's Procuratorate in 2017 published 'Interpretation of Several Issues concerning the Application of Law in Handling Criminal Cases of Infringement of Citizens' Personal Information'. According to Article 5, item 9, paragraph 1, those who have been subject to criminal penalties or administrative penalties within the last two years for violating citizens' personal information and illegally obtain, sell or provide citizens' personal information shall be deemed to have infringed upon citizens' personal information to the extent of constituting 'serious circumstances'.

## References

American Law Institute (2005) Model penal code and its commentary (Trans: Liu R etc.). Law Press, Beijing
Baker DJ (2011) The right not to be criminalised. Ashgate Publishing Limited, Farnham
Bentham J (1789) An Introduction to Principles of Morality and Legislation. The Commercial Press, Shanghai
Cao X (2019) The devil of the internet black industry being "One foot high", strict punishment and strict rules can lead to a higher moral compass. Science and Technology Daily
Chalmers J, Fiona L (2008) Fair labelling in criminal law. Mod Law Rev 71:217–246
Chen J (2023) Reconsidering the criminalisation of deepfakes - a perspective on the regulation of technical risks from AI. Taiwan Law Rev. 333:21–39
Chen X (2017) The value structure of criminal law, 3rd ed. China Renmin University Press, Beijing
De Hert P, Gutwirth S (2009) Data protection in the case law of Strasbourg and Luxemburg: constitutionalization in action. In: Gutwirth S et al. (eds) Reinventing data protection? Vol 2. Springer, Heidelberg
De Hert P (2014) The EU data protection reform and the (forgotten) use of criminal sanctions. Int Data Priv Law 4:262–268
Dimitrova R (2019) Criminal law protection of personal data - the experience of other EU member states. Contemp. Law 3:53–68
Dimitrova R (2020) Criminal law protection of personal data - Italy's approach. Contemp Law 4:27–42
Dove ES, Chen J (2021) What does it mean for a data subject to make their personal data 'manifestly public'? An analysis of GDPR Article 9(2)(e). Int Data Priv Law 11:107–124
Dubber MD (2015) An introduction to the model penal code. Oxford University Press, New York
Fan J (2023) The application of AI ChatGPT generation and Personal data protection. Taiwan Law Rev. 341:26–35
Feinberg J (1984) The moral limits of the criminal law volume 1: harm to others. Oxford University Press, Oxford
Gaagouch A (2024) The protection of personal data according to the civil and criminal Moroccan Laws in light of jurisprudence. J Data Prot Priv 6:240–255
Gal MS (2018) Algorithmic challenges to autonomous choice. Mich Technol Law Rev 25:59–104
Gao M (2012) The birth and development of the criminal law of the People's Republic of China. Peking University Press, Beijing
Gellert R, Gutwirth S (2013) The legal construction of privacy and data protection. Comput Law Secur Rev 29:523–525
Gon S, Li T (2022) Research on the path of Criminal Law Protection for the abuse of citizens' Personal Information - Taking Personal Health Information as an example. J Beijing Univ Aeronaut Astronaut 6:64–71
Guo Z (2023) Proportionality of communication record data retrieval. Glob. Law Rev 4:9–55

Guo Z, Hao J, Kennedy L (2024) Protection path of personal data and privacy in China: moving from monism to dualism in civil law and then in criminal law. Comput Law Secur Rev 52:105928
Guo Z (2024) On the risk assessment of preparatory behaviors. Peking Univ Law J 5:1303–1323
Hilbert M (2016) Big data for development: a review of promises and challenges. Dev Policy Rev 34:135–147
Hillenkamp T (2018) Where is victimology doctrine now? A summary of the "victimology criteria" as principles of legislation, interpretation, attribution and sentencing (Trans: Chen Xuan). Comp Law Res 5:180–200
Igo S E (2018) The known citizen: a history of privacy in modern America. Harvard University Press, Cambridge, Massachusetts
Jian Z (2022) The basic subject of article 41 of the personal data protection law "crime of violating personal information" - taking the review of the Supreme Court's Criminal Decision No. 1869 in 109 Year as an opportunity. Crim Policy Crime Prev Res Spec Issue 32:131–184
Kröger JL, Miceli M, Müller F (2021) How data can be used against people: a classification of personal data misuses. SSRN
Li C (2019) The regulatory dilemma of personal information crime and the improvement of countermeasures - starting from the problem of information abuse in the big data environment China. Crim Law J 5:34–47
Li H (2020) Criminal sanctions for misuse of personal biometric information - taking artificial intelligence "Deep Forgery" as an example. Political Sci Law Forum 4:144–154
Li Z (2019) On strengthening criminal law regulation of the illegal use of personal financial information. J East China Univ Political Sci Law 1:81–93
Li Z (2022) On the Criminal Regulation of Illegal Acquisition or Utilization of Facial Recognition Information. J Soochow Univ (Philosophy and Social Science Edition) 1:72–83
Lin Y (2019) The challenge of personal data law in the new era (Part II): starting from GDPR. Taiwan Law Rev. 287:210–227
Lin P (2023) White paper: infringing on citizens' "personal information crime happens, nearly forty percent for illegal and criminal activities". https://www.thepaper.cn/newsDetail_forward_25309743. Accessed 28 August 2024
Liu B (2022) Criminal law issues of personal data protection - taking digital footprint as an example. Leg Assist Soc 8:157–195
Liu R (2019) On the criminalisation of the illegal use of citizens' personal information. Law Forum 6:118–126
Liu S (2020) Criminalisation logic and exit path of the illegal use of personal information from the perspective of data compliance. Netw Inf Law Res. 2:86–106
Liu S, Li C (2022) The necessary shift of legal interests and criminal law protection of personal information in the era of big data: focusing on regulating the illegal use of personal information. J. Chongqing Univ 6:231–242
Liu X, Song Z (2022) On the regulation of the illegal use of personal information in criminal law. Juv Delinquency 4:64–73
Liu J (2020) On the statements of "Personal Information Protection Law of the People's Republic of China (draft)". http://www.npc.gov.cn/npc/c2/c30834/202108/t20210820_313092.html. Accessed 28 August 2024
Liu J (2010) Legislation that is not progressive: an initial assessment of the personal data protection act. Taiwan Law Rev 183:147–164
Loideain NN (2019) A port in the data-sharing storm: the GDPR and the Internet of things. J Cyber Policy 4:178–196
Lu D (2010) Analysis on the amendment of "personal data protection act". Taiwan Law Rev 183:131–146
Lu Q, Zhang Y (2023) Legislative conception of criminalising the illegal use of personal information. Hebei Law 1:73–96
Lynskey O (2015) The foundations of EU data protection law. Oxford University Press, Oxford
Ma K (2007) On the orientation of criminal policy of combining leniency with severity. China Leg Sci 4:117–122
Maeda M (2017) Lecture Notes on General Theory of Criminal Law (Trans. Zeng W). Peking University Press
McGlynn C, Rackley E (2017) Image-based sexual abuse. Oxf J Leg Stud 37(3):534–561
Miruć A (2013) Limits of the prohibition of using personal data of social assistance beneficiaries. Stud Log Gramm Rhetor 32:123–137
Phillips M, Dove E, Knoppers B (2017) Criminal prohibition of wrongful re-identification: legal solution or minefield for big data? Bioethical Inq. 14:527–539
Privacy International (2018) Invisible manipulation: 10 ways our data is being used against us. https://privacyinternational.org/long-read/1064/invisible-manipulation-10-ways-our-data-being-used-against-us. Accessed 28 August 2024
Prosser WL (1960) Privacy. Calif. Law Rev. 48:383–423
Ren Z (2024) Optimal application of fines for crimes of infringing citizens' personal information. China Price Regul Anti Monop. 8:111–113
Ribet C (2023) Don't just do something, stand there: what criminal law teaches us about article III standing in data breach cases. Univ Pa Law Rev 172:257–286
Shutova A (2022) Patients' personal data, including biometrics, as objects of criminal law protection. Int J Law Changing World 1:46–59
Staunton C (2021) Enabling the use of health data for research: developing a POPIA code of conduct for conducting research in South Africa. South Afr J Bioeth Law 14:33
Sun D (2012) Rethinking the protection law of criminal law. J Natl Acad Prosecutors 5:86–93
Sunstein CR (1996) On the expressive function of law. East Eur Constitutional Rev. 5:66–72
Tian J (2023) Illegal use of citizens' personal information should also be criminalised". Procuratorial Daily. 11 February 2023
Tong Y (2024) The linkage mechanism between the personal information protection law and the crime of infringing on citizens' personal information. Peking Univ Law J 2:366–385
Waldron J (2012) The Harm in Hate Speech. Harvard University Press, Cambridge, Massachusetts
Wang K (2017) On the General Personality Rights in the Constitution and Their Impact on Civil Law. China Leg. Sci. 3:102–121
Wang S (1999) Study on the interaction between economic policy, economic criminal law and economic crime in Germany. Peking Univ Law J 6:98–104
Wang X, Huang Z (2024) Network charity act or network violence: the boundary and legal control of network reporting and supervision. Law Forum 5:5–16
Wang Z (2015) Relativity of illegality judgment from the perspective of unity of legal order. Peking Law Rev 1:170–197
Warren SD, Brandeis LD (1890) The right to privacy. Harv Law Rev 4:193–220
Wen J (2023) Debate on the criminal law regulation of illegal use of citizens' personal information. Peoples Procuratorate 17:58–61
Xiao Y (2012) Legal problems in Taiwan's personal data protection act. Chenggong Univ Law J 23:141–191
Xue Z (2021) The concept of interest in the crime of infringing personal data — a comment on the Supreme Court's ruling no. 1869. Taiwan Law Rev 313:62–75
Zhang Q (2001) The Western constitutional system. China University of Political Science and Law Press, Beijing
Zhao B (2017) Review and prospect of Chinese criminal law legislation in recent 20 years. China Leg. Sci. 5:47–68
Zharova AK, Vladimir ME (2017) The use of Big Data: a Russian perspective of personal data security. Comput Law Security Rev. 33:482–501
Zhou H (2018) Exploring an incentive-compatible approach to personal information governance: the legislative direction of China's personal information protection law. Law Res. 2:3–23

## Acknowledgements

I would like to thank Dr. Jiahong Chen (University of Sheffield), Dr. Lewis Kennedy (Faculty of Advocates), Mr. Xiaoyuan Wang and Ms. Chen Jin for their sincere help during the preparation and revision of the article. Generative AI and AI-assisted technologies were only used in the writing process to improve the readability and language of the manuscript. This research is supported by Program for Young Innovative Research Team in China University of Political Science and Law (25CXTD09) and National Social Science Fundation Youth Program (23CFX065).

## Author contributions

Zhilong Guo wrote the main manuscript text and prepared diagram 1 and revised the manuscript.

## Competing interests

The author declares no competing interests.

## Ethical approval

The study does not involve human participants or their data. It is a doctrinal and policy analysis based on published legislation, cases and news reports.

## Informed consent

The study does not involve human participants or their data. It is a doctrinal and policy analysis based on published legislation, cases and news reports.

## Additional information

**Correspondence** and requests for materials should be addressed to Zhilong Guo.