US-China Law Review, July 2022, Vol. 19, No. 7, 312-327
doi:10.17265/1548-6605/2022.07.003

Research on Smart City Construction From the Perspective of Privacy Protection

WANG Dezheng
University of International Business and Economics, Beijing, China

As the core content of a smart city, data are related to citizens' personal information as well as to personal privacy and other corresponding rights and interests. The construction of a smart city relies on the collection and utilization of these data. Although data collection greatly improves urban governance and facilitates public life, the excessive collection and utilization of citizens' personal information have intensified the risk of infringement of citizens' personal privacy rights. The boundary between the public sphere and private space of individuals, and the virtual position of informed consent, has blurred. This infringement of personal privacy has changed from actual harm to "risk enhancement" infringement. In the traditional privacy protection mode, it is difficult to guarantee the protection of citizens' personal privacy in the big data society. By constructing an information track, and ensuring perfect digital rights management, we can ensure user empowerment of the right to self-determination and can govern digital evasion to promote the transformation from "digital humans" (i.e., people using digital technology while being controlled by it) to "digital *Homo sapiens*" (i.e., people using digital technology without being controlled by it). This transformation is a response to the need to overcome the data control and discrimination caused by monopolies on personal data held by the information industry and to balance the value conflict between data utilization and personal privacy protection in smart city construction.

Keywords: privacy right, digital *Homo sapiens*, data security obligations, digital evasion, digital governance

Introduction

A smart city is a visual and measurable intelligent city management and operation system established on the basis of the comprehensive digitalization of a city. Digitization includes city information, data, and infrastructure, as well as a networked city information management platform and comprehensive decision support platform established on this basis (Li, Shao, & Yang, 2011). To solve urban diseases and improve the modernization of the national governance level, the construction of a smart city has become a national strategy in China and has been actively promoted at the local level. According to the 2018 New Smart City Development and Practice Research Report of the China Academy of Information and Communications Technology, all cities at or above the subprovincial level, 89% of cities at or above the prefecture level, and 47% of cities above the county level have proposed smart city construction plans (Tang et al., 2020, p. 74). The construction of "a smart city" in some

Conflicts of Interest: The author declares no conflicts of interest regarding the publication of this paper.
WANG Dezheng, Ph.D. candidate, Law School, University of International Business and Economics, Beijing, China.

developed cities has been upgraded from digital Version 1.0 to intelligent Version 4.0, and is moving toward the upgrade of Version 5.0, which combines the metaverse and smart city (Tang et al., p. 74). Data collection, data mining, data analysis, and data utilization are essential for the construction of a smart city; however, this can represent a significant threat to the protection of citizens' personal privacy. Data are becoming increasingly personified, and individuals are being transformed from real people into digital identities. In the digital age, the information transparency caused by information sharing goes in an opposite direction to the protection of personal privacy. The privacy infringement of "digital people" in the construction of a smart city has changed from actual harm to "risk enhancement" infringement (i.e., an elevated risk). However, the generalization of this infringement is acute because of ineffective privacy protection resulting from the difficulty of judicial judgment.

Digital Oppression in the Construction of Smart Cities

In the prenet work information age, the relationship between personal privacy and personal information was not as complex as it is in the current digital society. According to the traditional concept of privacy, it is difficult to draw the conclusion that the knowledge and disclosure of personal information constitutes an invasion of personal privacy. As network information technology and the depth of social life have combined, virtual space and the connection between the physical world have become increasingly close and increasingly blurred. As a result, the relationship between personal privacy and personal information has become inextricably linked. The privacy of a digital society is like a chameleon "as the specific background and context of [a] different and constantly changing" environment (McLean, 1996, p. 3). The boundary between personal information and privacy is blurring. In the process of deepening the construction of smart city, what mode should be adopted for personal information and privacy protection? Academic opinion is divided (Jiang, 2022, p. 153).[1] Both academic and practical circles have looked for a way to protect the digital society that fits under the traditional framework of tort liability; however, this has further intensified the sense of incompatibility.

Survey of the Abuse of Citizens' Personal Information in the Context of Epidemic Prevention and Control: The Zhengzhou Red Code Event

Recently, a total of 1,317 depositors who opened accounts in Henan rural banks were given red health codes and their travel was restricted, which attracted widespread attention (Feng, 2022). Although the people involved in the incident have been held accountable, many concerns about its impact on the society have not been eliminated. In particular, the subsequent disclosure of the involvement of the investigating body and the initiation of the investigation further fermented the case: Is it legitimate to apply the health code, which is designed for a specific purpose, and use that code based on a major epidemic as control method for other events? In a word: When personal information collected for a specific purpose is used for other purposes, which regulations should be applied?

The outbreak of the COVID-19 pandemic has tested the national modern governance capability against the backdrop of smart city construction in China. In the face of this threatening new epidemic, and under the guidance

[1] Five stages of smart city: 1.0 Version of Smart City, focusing on digitalization; Smart City 2.0, featuring the "Internet of everything"; Smart City 3.0 Version, with "intelligent" and "big data" to enable the core; Smart City Version 4.0, characterized by wisdom; Smart City Version 5.0, smart city and meta-universe combined, virtual space brings people more possibilities and enables the development of the physical world.

of the government, all parts of the country were provided with technical support for government departments to obtain epidemic data in a timely manner. Governments obtained real-time information through big data sharing, epidemic intelligence consulting service platforms, epidemic maps, and public opinion monitoring, and other technical means. This effort effectively improved epidemic prevention and control capabilities and optimized public service quality. The use of various technical means, such as “travel by code”, “online office”, and “remote approval”, effectively alleviated the negative impact of the epidemic. With improvements in epidemic prevention and control, the original technologies used for epidemic prevention and control have faced the risk of being misused in the post-epidemic era, which seriously infringes on the personal rights and interests of citizens, endangers social order, and affects social credibility. The weaknesses of related top-level design, construction management mode, and data management, including smart city construction, have been exposed. Users now face corresponding information security problems at different stages of information generation, dissemination, storage, and use, and thus the risk of privacy infringement has emerged in this digital economy era.

Information Generalization Behind Smart Cities

The new digital and intelligent technology has been comprehensively promoted. Every individual, whether actively or passively, has been involved in this technology onslaught without exception. Without acceptance, this new form of intelligent technology will be abandoned, leading to digital oppression. From daily code scanning and order counting, appointments, and registration, to travel ticket purchases, shopping, and delivery, any individual who cannot use new technology will meet roadblocks. Both technical discrimination and passive technical resistance are behind this digital oppression.

In a digital society, personal information rights and privacy protection are faced with a dilemma. To protect their personal rights and interests, people have to give up corresponding technologies, or people must use these new technologies at the risk of infringement of their rights and interests. This requires a huge adjustment as well as abandoning the social style, lifestyle, and working style that individuals have become accustomed to. This can have a profound impact on the individuals, who face risks and difficulties that may be difficult to adjust to. According to Marcuse, as technology becomes a dominant ideology, it gives people comfort and enslaves them (Marcuse, 1988, p. 25). Under this form of digital oppression, the collection, storage, and application of personal data information as well as the monitoring, recording, and abuse of personal information go hand in hand. This is the inevitable result of improving urban governance capacity and modernizing the governance system to promote the integration of cities and digital technology. When digital technology penetrates the social space comprehensively and deeply, all individuals in the smart city are likely to fall into a circular prison (Major, 2021, p. 37).

Generalization of information collection subject. In the digital economy era, along with the diversification of reasons for the collection of individual information, the entities of information collection are also following a generalization trend. The entities collecting information range from different government departments to enterprises, institutions, and other commercial institutions or other organizations. Because of the generalization of collection entities, the network supervision has faced a phenomenon known as the Kowloon Water Control (Liu, 2018, p. 61). The construction of smart cities has lacked intelligent synergy, and an information island effect (i.e., a computer application system where information is not shared or exchanged, and is disconnected from business processes and applications) has become obvious, which has resulted in unclear

rights and responsibilities, low efficiency, and other problems. A system to ensure subject responsibility is lacking, and any negligence of enterprises and various national regulatory departments may lead to a bucket effect, resulting in a failure to protect personal information and privacy.

Collection information content generalization. The use of personal information is extensive in a networked digital society, and any aspect of personal information may be used for a variety of purposes. This personal information includes fingerprint punching, face recognition, and QR code scanning. From basic personal information, such as name, gender, and date of birth, to education background, work experience, and family situations, as well as personal address books, income, health, photos, and other information, individuals may be required to provide data on various occasions. Many different types of information, such as personal consumption patterns, travel paths, personal hobbies, and health status, are collected. This additional accumulation of relevant data to form a huge information space (i.e., the data sea) is an inevitable trend in the development of smart cities. The challenges facing confidentiality, integrity, authentication, reliability, and other aspects of information are intensified. For example, Didi Company, which recently was fined a large amount, has overcollected and abused personal information in the process of providing online car-hailing services for customers. Didi illegally handled 64.709 billion pieces of massive personal information. The information includes accurate location information, including 153 million pieces of taxi location information of "home" and "company", 167 million pieces of accurate location (longitude and latitude) information obtained when the mobile phone is connected to the orange video recorder, ID card numbers (including 57.8026 million pieces of driver's ID card number information stored in clear text), 142,900 pieces of driver's personal education information, 107 million pieces of face recognition information, 53.5092 million pieces of age-group information, 16,335,600 pieces of occupational information, and 1,382,900 pieces of family relationship information. In addition, 11,963,900 pieces of screenshots from users' mobile phone photo albums were illegally collected, and more than 8.323 billion pieces of user clipboard information and application list information were collected. Data contained a variety of sensitive personal information. Didi also cannot give a clear and accurate description of 19 personal information processing purposes such as user equipment information.[2] The launch of Didi's car hailing service undoubtedly facilitates people's travel and provides employment opportunities for relevant practitioners; however, while accessing these conveniences, users are forced to give up control of relevant personal information, which seriously endangers the security of personal information.

Generalization of the purpose of collecting information. The use of personal information ranges from daily basic necessities of life to medical education and employment. As a result, it is collected, and then misused, which is but one of the most common ways that personal information is infringed upon. The public management and commercial value of personal information has created a huge incentive for public and private institutions to improperly collect, process, use, and transmit personal information (Zhang, 2015, p. 47). As mentioned earlier, Didi Company overcollected user information, and used algorithm technology to reason and analyze the passenger's travel intention information without notifying its customers. Data collection reached 53.976 billion pieces. In addition, Didi has conducted mining and analysis on the passenger's resident city information (1.538

[2] From the WeChat official account "Governor of Chang'an Street", "Finding out 16 Illegal Facts, Didi Will Be Fined RMB 8.026 Billion", July 21, 2022, https://mp.weixin.qq.com/s/lhTD738rvW0GQnFxUtkQ8Q, last visited on July 22, 2022.

billion pieces) and long-distance business/tourism information (304 million pieces). This algorithm operation is an example of the improper collection and abuse of personal information.

Admittedly, the diversity and diversification of choices promote the better satisfaction of personalized needs, but this comes at the cost of the transfer of personal confidential information. The higher the satisfaction of needs means the higher the degree of personal information being collected and mastered. The information subject is facing not only the risk of personal privacy disclosure but also the risk of losing the right to choose because of an insufficient right to know about personal information consumption products and services (Wei, 2015, p. 77). The price paid by users to enjoy relevant services exceeds expectations, which is called a "Faust transaction" in the digital economy era (Famularo, 2020, p. 38). It is also the inevitable result of a data monopoly. Even for the legally collected personal information, the processor, based on the big data thus formed, conducts social sorting, discriminatory treatment, and completely automated decision-making through algorithms and other technologies, which will also damage the risk of human dignity and personal freedom (Winfried, 2018). In light of such personal information abuse, the question is "Which governance options should we choose?" In the new digital economy, the rejection of digital technologies is tantamount to self-isolation, and the choice of new digital technologies is faced with the risk of streaking, facing a new digital era in which the rejection of new technologies means death (Flandin, Gramon, & Cox, 2020). Data governance is a rational measure for the times. Data governance means that we need to build a new management mechanism of making decisions with data, managing with data, and innovating with data against the reality that information data are abused.

Privacy Protection Problems of a "Digital Person" Under Digital Oppression

In a smart city, the core function of big data is prediction and reasoning. With its superior ability to collect, store, timely and accurately process data, and make accurate predictions, big data can extract more value by mining, collecting, analyzing, inferring, and "sketching" the intent behind the data through known information. In addition to the necessity and legitimacy of big data in criminal investigation, information analysis and behavior inference prediction in other fields also requires ethical reflection. For example, considering the most common application of personalized consumer advertising, following personal consumption, input, and retrieval of certain item information, big data pushes relevant product sales information to individuals. This kind of prediction of consumption habits, consumption trends, and consumption levels provides convenience for consumers, but it actually constitutes a hindrance to the right to self-determination of personal information, and has characteristics of algorithm bias and algorithm discrimination. This practice also involves sensitive information that individuals may not want to be known by others. If an infringement has occurred, individuals may not be aware of the fact that their private information has been shared. Although legislation has given many provisions to protect personal information, under digital oppression, technology empowerment has been insufficient and supervision has been weak. The protection given to digital people faces the risk of infringement. Behind all intelligence is monitoring and control (Sadowski, 2020). Under digital oppression, people cannot effectively deal with the lack of digital privacy while also enjoying digital convenience. The choice of "technology resistance" based on personal information security and privacy protection inevitably will restrict the adoption of technology.

Debate Between Personal Privacy and Personal Information

To promote the construction of smart cities, governments have made full use of various emerging technologies. While working to achieve the goal of benefiting, profiting, and facilitating the people, it is inevitable that the negative effects of technology use will occur. The greatest victory in technology is almost equal to the greatest disaster (Kun, 2002). Does the general promotion of digital intelligence technology enable individuals to freely access technology? Alternatively, is this access to digital technology a trap? Digital people in a digital society face the confusion of whether it is technology empowerment or technology binding. All types of infringement events caused by improper disclosure and illegal use of personal information have aroused people's awareness of rights. The widespread promotion of new technologies, such as face recognition, track recording, and video surveillance, also has compelled people to pay attention to private personal information. The current understanding of personal information and privacy, however, remains vague. The public often uses them as substitutes, and the academic community also has its own views on personal information and privacy.

Value choice between inclusion theory and independence theory. With the promulgation of China's Civil Code and the Personal Information Protection Law, the content of privacy and personal information has aroused academic debate. Thus, two different views have been formed: inclusion theory and independence theory. Researchers who follow coverage theory believe that the Personal Information Protection Law is actually a privacy protection law. There is no difference between the protection of personal information and the protection of privacy. The unique value of privacy is the only basis for personal information protection (Chen, 2022, p. 38). The right to privacy includes the rights and interests of personal information. Thus, privacy is the only reason to protect personal information (Xu, 2017). Researchers who hold the independence theory, however, believe that the rights to privacy and personal information rights and interests pertain to two independent specific personality rights and interests, which are neither mutually substituted nor mutually inclusive (Cheng, 2022). Given that data information is the core content of a smart city, does the collection of personal information inevitably face the risk of privacy protection? The academic circles have paid attention to this question, and the corresponding arguments reflect the different value orientations behind the system implementation. The development of "personal private information" from the integration of personal privacy and personal information leads to the conflict of departmental norms and difficulties in its legal application, which further aggravates the complexity of judicial practice and gives rise to more complicated problems. From the foreign personal information and personal privacy protection situation, single protection and dual protection models can be applied. The specific handling of data in practice is also different. These kinds of cognitive differences and different practices aggravate the practical difficulty of ensuring personal privacy and information protection.

Personal information and personal privacy in the digital society. At present, China's legislation on personal information and privacy has been established as a dual protection model. Although the identification of the relationship between personal information and privacy is still disputed, it is certain that in the digital information society, the two overlap and are integrated, which can be called information privacy. The development of information technology has increased the difficulty in distinguishing between privacy and personal information (Xu, & Sun, 2021). It generally is believed that personal privacy is the private part of personal information, but this so-called privacy is actually relative—that is, the privacy of information is related to the range of audiences

that individuals allow to access their information content. In other words, some personal information of citizens, such as educational experience, professional background, identity information, and family members, may agree to be known or shared by others within a limited range. The disclosure of information beyond the scope of what they allow constitutes an infringement of privacy. In other words, privacy is a boundary with self-imposed limitations, which requires a combination of a series of secondary rights and interests (Xu, 2017). The right to privacy means that individuals have the right to determine the extent to which the public can access their thoughts, feelings, private behaviors, and private affairs (Godkin, 1890). The cumulative impact caused by this continuous collection of personal information will cause individuals to lose control over the scope of the audience to which they have consented. This leads to the risk of privacy infringement as a result of the disclosure of personal confidential information. Thus, big data has greatly expanded the depth, breadth, and severity of privacy violations (Xu, 2017).

In the age of big data, information will spill over the traditional field and enter the stranger relationship of the noncommunity (Fang & Cao, 2019). This practice has exceeded the original cognitive category of privacy. Non-private information also has become part of the right of privacy under specific conditions, and it cannot be disclosed or used improperly. For example, Pang Lipeng sued China Eastern Airlines Co., Ltd. and Beijing Quna Information Technology Co., Ltd. over a privacy dispute. The people's court concluded that the information leaked by the plaintiff Pang Lipeng included his personal name, real name registered mobile phone number, specific itinerary, and other information. Although this specific personal information had nothing to do with personal privacy, the combination of this specific information undoubtedly allowed entities to "visualize" specific personal activities, which should have been treated as private information. "Digital personification" is caused by the accumulation and summarizing of information, which may bring trouble, unease, embarrassment, and even shame, which are some of the problems faced by digital people due to privacy infringement. The personal information that appears to be fragmented can show a broad perspective when it is accumulated through a specific collection and analyzed using corresponding algorithm technology (Xu & Sun, 2021). Even if individuals lack the cognition and psychological expectation of privacy protection for this fragmented information, when a large amount of information accumulates it can lead to personal digital personification. Thus, it still poses a considerable risk to personal privacy infringement.[3] Metaphorically, personal privacy is to its information as clothing is to the human body, creating an inevitable relationship between the two.

Nonintelligent Protection Risk of the Smart City on Personal Privacy

The efficiency and convenience of a smart city reflects its "smart" purpose. In the process of effectively operating a smart system, given the fuzziness of public and private fields and the weakening of the reasons for informed consent, the protection of citizens' privacy presents the risk of "nonintelligent protection".

Fuzzification of public space and private space. In the pre-network information society, the recognition of privacy usually was related to the public sphere and the personal private space. In this case, public and private can be defined according to specific visible and perceptible traditional physical space. Individuals have relatively active control over their living space, and thus, it is fully reasonable to take the "public sphere and private space as the core of building privacy" (Turkington & Allen, 2002, p. 1). With the transformation from a "perceived

[3] United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010).

physical space" to a "digital city", in a highly open, high-speed information flow and an interactive virtual network world, the boundary between public and private fields has become blurred. Any network an individual accesses will leave traces, which can enable the collection of individual private information. Individual fragmented information will be integrated unconsciously and gradually form a "personality profile" (i.e., the digital person). Individuals who turn into digital people may not be aware and thus cannot control the use of their personal information when other entities interfere. The secrecy of the intervention has changed privacy violations from having specific harmful consequences to having a risk of infringement. The traditional practice of "privacy ends [at the] front of the door", which used the physical controllable space as the boundary of privacy protection, has become difficult to maintain in a digital society in which data consumption and sharing have become ingrained. In other words, it is not appropriate to simply take the public sphere and private interests of material rationality to define privacy in a digital society.

False notification of informed consent. When considering privacy with autonomy of will as the core tenet, informed consent can constitute a legitimate defense against infringement as long as it does not violate the mandatory provisions of the law or public morality. Voluntary hindrance (i.e., with the consent of the victim, some injuries such as collecting, storing, and utilizing the personal information are not illegal) (Zhu, 2011, p. 497), which takes the informed consent of civil subjects as the defense, can work in traditional privacy infringement cases, but it faces significant challenges in the digital society. In the age of big data, the principle of informed consent for the privacy agreement set by the network operation service enterprise is not sufficient to protect personal privacy, and it is difficult to effectively protect personal privacy (Wang, 2022, p. 84).

The logic of the data protection law for citizens' privacy is based on informed consent. Practice shows, however, that few users seriously read the privacy terms carefully set by service providers, particularly when faced with redundant electronic terms, not to mention the vague and unpredictable terms of the relevant privacy terms. More reluctantly, earnest users are faced with a dilemma after reading the relevant terms to protect their own rights. They either give up use based on the protection of their own rights, or transfer the corresponding rights based on the needs of use. The user does not have veto rights to the informed consent clause, which means that the user cannot continue to use the corresponding software without granting consent. Whether or not the user gives informed consent has become a unilateral exemption clause. The user has the right to deny the corresponding authority, and it seems that the user has the right of self-determination to agree or disagree with the specific authority required by the corresponding software service. Once the user opts to limit the corresponding authority, however, it leads to a limitation in use of software functions and to a poor experience with software use. Therefore, whether or not it is accepted, the user eventually must accept the informed consent notification clause if they want to use the application. The informed consent notification clause thus has been reduced to a zombie clause, which "causes the network users to lose effective control over personal information and personal privacy" (Ji, 2017, p. 22), thus transferring the user's right to self-determination to the supplier.

System Adjustment of the Transformation From "Digital Human" to "Digital *Homo sapiens*"

The "digital *Homo sapiens*" is used to define a digital personality that has self-determination toward the use of digital technology. By embracing new technology rather than resisting new technology, and making use of

new technology rather than being trapped by new technology, the digital human can be transformed in the "digital *Homo sapiens*", thus maintaining human's subjective initiative and value-centered characteristics in digital governance. The smart city itself is not smart, but the key lies in the public value it creates for people (Liu & Li, 2019). The protection of data information ensures human dignity for individuals and provides for basic societal justice. The sustainable and healthy development of smart cities should seek a balance between citizens' personal privacy and the public value they create. We should not only avoid the irrational choice of "data avoidance" but also ensure the security of citizens' personal information and privacy. "Smart cities need to be" people-oriented and "explore sustainable development models to serve the city" (Wu, 2014, p. 10). The protection of personal privacy and the protection of information security reflect the basic requirements of a "people-oriented" city. The risk of personal privacy being violated includes the risk of violating personal information security. Fundamentally, the protection of personal privacy needs to begin with information security prevention and control. We should combine social management with science and technology, and focus on situational conditions, governance models, personal information, and public values (Meijer, Gil-Garcia, & Bolívar, 2015). Two different levels of technology and law should be applied to address the current privacy dilemma.

Building an Information Track: Standardizing the Flow of Information

In the smart city information ecosystem, the smart city covers many elements, including people, information, technology, and systems. As a typical information ecosystem, a huge amount of information is generated and transferred in the operation of the smart city (Mao, Huang, & Xu, 2019, p. 124). It is difficult to draw a conclusion that such information is irrelevant to personal privacy. In particular, the blurring of the boundary between public field and private space has led to the weakening of an individual's dynamic control over private space and public space. The blending of personal information and privacy and the controllability of individuals to this information flow have been weakened. The right to privacy has extended into a dynamically balanced scope, and interests in data and information are diversified, resulting in complex conflicts of interest. Data loopholes, digital control, cybercrime, data abuse, and data hegemony have all buried security risks in the city base that relies on information operation (Wu, 2022, p. 71). A digital city is not only a space to gather various information flows, but also a space to gather more complex and contradictory flows. It is difficult to effectively protect personal privacy by framing the privacy boundary of a "digital people" within the public sphere and a personal private space.

The generation, collection, storage, and circulation of information all have specific rules. The privacy protection of smart city construction should not only follow the objective laws and procedures of digital technology, but also should follow a technical code according to the needs of privacy protection. By standardizing the corresponding code rules, we can build an invisible information track and standardize the flow of information to ensure the security of personal information (Staddon, 2003, p. 94).

Only by "jumping out of the 'information content' and turning to the 'processing behavior', starting from the three factors of the type, specific occasions and consequences of processing information, and combining with specific scenarios to study and judge" (Xu & Sun, 2021, pp. 12, 15, 16), can we identify and define whether or not personal information is related to personal privacy. We must ensure that personal data information can be transferred to an information track in a way that is controllable. Through the specification of the corresponding computer code rules to build an invisible information track, we can control the operation of information

specification to avoid the consequences of the flow of data information getting out of control. We must set traffic runways to maintain the order of smart cities to ensure personal privacy. The construction of a smart city should not only achieve thorough perception, connectivity, and in-depth intelligence in technology but also achieve comprehensive wisdom in residents' lives, urban economy, and management (Gu & Wang, 2012). By taking the controllability and legal interference of information as the entry point of personal privacy protection, we can determine the status of personal information on the information track. We must place personal information specifications on an information track to achieve effective supervision. This is an important condition to ensure information security to guarantee that personal information runs in a standard and orderly manner along the information track.

Perfecting Digital Rights Management: Eliminating Risk

Whether or not data information can flow in an orderly and controllable manner on the information track is closely related to the authority enjoyed by the information holder. It is an important link to ensure information security to standardize and coordinate the interest expectations of the three parties associated with data (i.e., data enterprises, users, and competitors in the same industry), clarify their respective authority on data information, determine the boundary of commercial use of data information, and subdivide the innovation governance of commercial tracks. In the risk-oriented network environment, the power to formulate and implement relevant digital technology rules tends to be decentralized. In the reconstruction process of the decentralization of power from the state to social organizations, an "artificial risk" is caused by the different enforcement of rules and the interest induction, which increases the difficulty of information management. The protection of digital security is closely related to the management of data rights. Perfect digital rights management is an important condition for the transformation from "danger prevention" to "risk prevention" and also is an important path for the transformation from tort relief to risk prevention and control. The effective implementation of digital rights management (DRM) to prevent a new type of privacy infringement called "ideological peeping" is essential to protect the right to privacy in the digital society.

DRM is an important aspect of smart city construction. It protects the corresponding digital content of the content provider by encrypting the digital content and requiring the consumer to obtain a license to use the content. DRM also includes other regulatory technical means to avoid the illegal use of the corresponding digital content. The most prominent feature of big data application in smart city construction is the loss of information subject's right to self-determination because of the transfer of information, which leads to the elimination of the right to confidentiality and control of personal information. The improper use of big data "seriously damages the dignity of individuals and the subjectivity and integrity of human beings" (Ren, 2017, p. 60). The protection of user data confidentiality is related to privacy and information security in the construction of smart cities. Information storage is closely related to personal information security. According to the requirements of the "right to be forgotten" clause in EU data protection, the information holder has the responsibility to delete citizen information in a timely manner after completing service, to "inhibit and delete the right to access information" (Garside, 2014). China, however, currently lacks mandatory provisions on the deletion or anonymization of data information, and no corresponding basis for the "right to be forgotten" exists. As a result, the information collected for exclusive use has been stored and improperly used. This is why Didi APP was taken off the shelf

and subsequently incurred huge fines. This kind of ex post facto punishment is not conducive to the early prediction and prevention of risks, and it is difficult to avoid the recurrence of similar events. The emergence of blockchain technology provides a new path for data protection. Through blockchain technology, the ability to identify, evaluate, and prevent risks can be strengthened. According to the decentralized and tamper-proof functions of blockchain distributed accounting, this technology can be fully used to strengthen the protection of citizens' information. Improved data compliance management will promote the structure and standardization of data processing to prevent the risk enhancement of privacy violations.

User Technology Empowerment and Technology Empowerment

As a tool to serve people, the digital technology of smart cities should not become a weapon used against individuals. The reason why the network has some effect and power to control human behavior is that people have given the corresponding power and autonomy to the network digital technology (Lu, 2020). In the face of digital oppression, to ensure individuals become digitally intelligent people and to fully protect personal privacy and information rights, it is necessary to give users a full sense of self-determination through technology empowerment. People must have the right to freely decide the extent to which the world around them knows their thoughts and actions (Steinmuller et al., 1972). We must protect their "personality" and "personal personality" in the process of using technology to ensure that their confidentiality will be fully respected and guaranteed. As the basic protection paradigm of data processing activities, the informed consent framework, which is based on the informed consent or disagreement of users, jointly outlines the dynamic boundary of data subjects in data processing activities, so that the purpose of data processing activities is anchored within a reasonable range (Tang, 2021). Informed consent is the effective exercise of the right to self-determination and is the basic criterion for collecting information. Through informed consent, individuals can prevent information providers from using their personal information for purposes other than their authorized use without their consent, or providing their information to others for purposes other than their authorization (Zhang, 2019, p. 2).

Because users generally do not read the informed consent notification terms, and only click habitually to enter the next step of operation, it is necessary to clarify the motivation of this operation. In fact, even though users do not read these terms it does not mean that they do not attach importance to the rights corresponding to the corresponding terms. Instead, it means that the relevant terms are too complex and difficult to understand. Relevant clauses need to be simplified to enhance readability and understandability, and the user's ability to move onto the next step should be constrained by setting a specific amount of time to read the corresponding clauses. Terms that are not read within the specified time will not move onto the next step. For some important matters, corresponding answer options should be provided. If the user answers incorrectly, they would be denied the right to proceed to the next step. For example, China's antifraud center platform has set up similar operations for transfers such as Alipay. For users' initial transfers and transfers from unfamiliar accounts, they have to answer questions about corresponding situations that could be suspected of fraud. If the user answers incorrectly, they cannot transfer money, which reduces the risk of fraud to a certain extent. This technical design will affect the user's experience, to some extent, but based on the necessity to protect private information, the necessity of this operation should not be overlooked. In other words, when users access various intelligent technology services, they should also fulfill the relevant requirements of positive consent and substantive consent—that is, they should

pay attention to the content of personal privacy clauses, actively read, and understand their impact on personal rights and interests, avoid the appearance of negative consent and formal consent, and perform due diligence to protect their own rights and interests. It is essential to promote the efficient governance of smart cities through high-quality participation of multilateral entities. Only when the obligations of relevant parties are truly implemented can the information industry invoke the informed consent notification clause as a defense against infringement. The freedom of expression of individuals in informed consent notification must be fully guaranteed, and the "package consent" notification method must be avoided to ensure that individuals can accurately predict corresponding risks. This approach would fully guarantee that individuals have the right to decide when, to what extent, and in what way their information is known and communicated with others (Westin & Alan, 1968, p. 166). Of course, because of the particularity of privacy protection, informed consent notification, as a basic criterion, does not exempt information providers from other requirements. In other words, when information providers collect personal information, they also should abide by the principle of purpose and the principle of necessity.

Legislation Connection and Adjustment

In the construction of smart cities, technical improvements and rule optimizations with code governance ensure citizens' privacy; however, "technology cannot fundamentally solve the problem of information security and privacy protection" (Zhang & Zhou, 2016, p. 26). The protection of privacy cannot be separated from the protection of corresponding laws, thus establishing a dual-protection mode of law and code. Data information in the construction of a smart city has the orientation of many different legal departments, such as organizational law, behavioral law, and information law. It is difficult to fully protect the rights and interests of personal information and its privacy with only one law, which involves the convergence and coordination of laws of various departments, as well as the legislative response to the defects of current legislation. To balance of legal interests, however, legislation is a process of recognizing and expressing interests. To adjust various interests, the law needs to understand and understand different interests first (Guo, 1997, p. 10). In other words, legislation should consider the protection of rights and the promotion of technology application to avoid falling into the vortex of "computer bureaucracy" (Lu, 2020, p. 26).[4] Against the backdrop that relevant intelligent services have multiple meanings of "government platform", "automatic administration", and "data governance", it is necessary to balance the relationship between "rationality of technology application" and "legitimacy of administrative management" to regulate the exercise of digital technology power and to constantly explore new protection and treatment methods in digital governance.

At present, three different department laws of the civil, criminal, and administration law in China have established corresponding protection models for personal information protection. Specific data governance, however, has problems such as unclear regulatory authorities, the need to improve core supporting mechanisms, and the lack of specific measures for the legal use and security management of data. In practice, differences in understanding have resulted in differences in judicial practice of privacy protection. The connection, adjustment, and legislative response among the laws of various departments have yet to be implemented. In particular, the

[4] The so-called "computer bureaucracy" can also be called "intelligent bureaucracy". It is a phenomenon of extensive use and misuse of digital technology "power". It originates from the out of control, imbalance, and disorder of social (administrative) and interpersonal communication behavior of network digital technology.

current relevant legislative provisions and research countermeasures are slightly abstract. The research on privacy protection in digital society has focused on such aspects as principles and jurisprudence, and response to existing problems in the specific provisions of the current legislation in terms of privacy protection is insufficient. In essence, the protection of the privacy right of smart cities is established in the governance of digital codes. In an algorithm society based on the Internet, computer code is the law of the digital society. This code regulates the operation of algorithms to design a special code-based regulatory system (Lesge, 2009, p. 16). For the purpose of digital code compliance governance, the trend of future legislative development is to upgrade the code rules designed in digital code governance to establish national legal norms through legal procedures. As a result, this would effectively restrict the algorithm power (i.e., the ability of users to know an algorithm's purpose) through the rule of law and the rule of code, thus providing a privacy protection barrier for smart cities. As a systematic project, smart city construction needs to "consider and design all aspects, levels, participation forces, positive promotion factors and negative constraints of the entire architecture in an integrated way" through a national top-level design (Zhen & Qin, 2014).

Law Enforcement and Supervision

The protection of citizens' privacy requires not only the improvement and optimization of relevant technologies but also the guidance and supervision of the proper use of technologies. Against the backdrop of unequal status, the user's "right to self-determination" in the absence of regulatory safeguards can easily create "digital avoidance" for information industry operators. This so-called digital avoidance of responsibility refers to the empowering content that is equal in form but unequal in substance. The information industry uses its dominant position of unequal power to control digital technology, thus avoiding its legal responsibility to protect personal information. At present, the most common phenomenon is that the use of various application software, public accounts, applets, and other intelligent services is based on the access to basic personal information, such as user nicknames and avatars. According to the requirements that information collection should conform to the principle of legitimacy, relevant service providers should explain exactly why they are collecting the information. In practice, relevant instructions are extremely complicated, which leads to obstacles to users' understanding, or explanations are missing. If the user does not agree to obtain the corresponding permission, he or she cannot browse the relevant content or use the relevant software. In response to this common phenomenon, the country more relies on the relevant industry standards to adjust. Because of the lack of punishment measures and insufficient punishment, the corresponding information acquisition and notification methods essentially have been alienated to the means of "digital accountability" for information providers. The governance dilemma faced by data governance should be effectively addressed.

A supervision center for all kinds of applications and other technical software should be established by the government. Users can provide feedback or complain about the application and other technologies through the supervision center. The supervision center should verify the corresponding situation and determine the next handling measures. At present, China's primary response is to review the privacy protection of the corresponding services through a special review and take the unqualified services off the shelf for rectification or even impose a fine. The high penalty system for illegal handling of personal information established in China is the need to protect the personal information rights and interests of natural persons, safeguard public interests and social order,

adjust the unbalanced enterprise and individual forces, and regulate the Internet competition ecology (Sun, 2022, p. 22). To regulate illegal use by means of fines, which is mandatory and not beneficial, makes the information collector lose more than he has gained and thus curbs the illegal use of information collectors. The current mobile governance mode has created the suspicion that it is difficult to resolve these problems. The regulators cannot match the information industry in terms of information sources and technical strength and also face the high cost of regulation and supervision, which has led to its failure to operate normally.

Personal information includes personal freedom, business value, and public management value, which is closely related to public interests and national security. The use of personal information has become distinctly social, and the ability to protect personal information has gone beyond individual self-determination. Didi failed to perform its personal information protection obligations in accordance with the provisions of relevant laws and regulations and the requirements of regulatory authorities, and its excessive collection and illegal use of users' personal information seriously infringed on China's network security and data security. This event fully shows that based on their technological advantages, technology providers can determine the inequality between them and users in information decision-making power, and this leads to the transfer and deprivation of the right to self-determination of personal information. When the material result of risk is converted to structural attribution, it is necessary to trace the source of these structural factors caused by risk and seek solutions (Cong & Ren, 2012). To achieve digital compliance governance, information providers must improve their ability to predict, prevent, and respond to risks, and achieve collaborative governance with national regulatory authorities. The construction of a regulatory platform that integrates technical standards and legal rules would ensure the balance between data flow and data security. The use of data value should not be restricted because of privacy concerns, and the protection of privacy should not be ignored in pursuit of data value.

Conclusion

The application of digital intelligent technology has profoundly changed human life, and smart city construction remains in the initial stage of development. Judging from the current institutional response to smart city construction, smart city is still in a concept of attention but in practice there is no systematic specific countermeasures. The construction of smart cities faces with many uncertainties, including the arbitrariness of data control and use restrictions, which has caused social, political, and legal problems far beyond the technical field. As a systematic project in the construction of a smart city, the protection of citizens' right to privacy must be promoted at multidimensional levels, such as product equipment, technical support, management measures, and laws and regulations. To avoid the smart city trap, it is necessary to properly handle these privacy risks in the development process of smart cities; achieve smart governance of technology; and adopt a humanistic, smart mind supervision mechanism to make up for the defects of smart technology governance under pure digital governance. Thus, it is essential to achieve the security and controllability of network and information core technologies, critical infrastructure and information systems, and data in important fields. Technological innovation is moving in the right direction, but it also has a long way to go.

References

Chen, J. H. (2022). Value uniqueness of privacy: Why should personal information be protected? *Global Legal Review, 44*(1), 36-52.

Cheng, X. (2022). On the relationship between personal information rights and privacy rights. *Contemporary Law, 36*(4), 59-71.

Cong, Y. F., & Ren, C. H. (2012). From material results to structural attribution—A path analysis of urban risk research paradigm. *Frontier, 34*(5), 109-112.

Famularo, A. (2020). Trends and overall situation of data governance in 2020. In *Internet economy report* (Z1, p. 38). erWin.

Fang, S. K., & Cao, X. J. (2019). On the privacy essence of personal information personality interests. *Legal System and Social Development, 25*(4), 99-120.

Feng, H. (2022). People sit at home, the red code heaven, why the group of the group of Henan depositors were forced to change code. Retrieved July 18, 2022 from https://mp.weixin.qq.com/s/F4oZM4afahT-XZFMcDIXeA

Flandin, J. P., Gramon, G. M., & Cox, S. Q. (2020). *Digital disruption*. (J. Feng, Trans.). Beijing: Oriental Publishing House.

Garside, J. (9th September 2014). Right to be forgotten is a false right: Spanish editor tells Google panel. *The Guardian*. Retrieved from https://www.hitc.com/en-gb/2014/09/10/right-to-be-forgotten-is-a-false-right-spanish-editor-tells-goog/

Godkin, E. L. (July-Dee. 1890). The rights of the citizen, IV: To his own reputation. *Scribner's Magazine, 8*(1), 65.

Gu, S. J., & Wang, M. (2012). Theoretical thinking and strategic choices for smart city construction. *China's Population, Resources and Environment, 22*(5), 74-80.

Guo, D. H. (1997). On the distribution and regulation of interests in legislation. *Xiangjiang Law Review, 2*, 10.

Ji, L. L. (2017). Comparative study on legislative paths of personal information protection. *Library Development, 40*(9), 19-25.

Jiang, C. L. (2022). Metaverse and the future of smart cities. *Smart Buildings and Smart Cities, 29*(6), 153-155.

Kun, H. (2002). *World ethics conception*. (Y. Zhou, Trans.). Shanghai: Xinzhi Sanlian Bookstore.

Lesge, L. (2009). *Code 2.0: Law in cyberspace*. (X. Li & W. W. Shen, Trans.). Beijing: Tsinghua University Press.

Li, D. R., Shao, Z. F., & Yang, X. M. (2011). Theory and practice from digital city to smart city. *Geospatial Information, 9*(6), 1-5, 7.

Liu, J. R. (2018). Review and prospect of supporting legislation on the first anniversary of the implementation of the network security law. *China's Information Security, 9*(7), 59-62.

Liu, S. Y., & Li, S. R. (2019). Smart city governance: Reshaping the government's public service supply model. *Social Sciences, 41*(1), 26-34.

Lu, J. (2020). Analysis on the technical regulation and motivation of intelligent bureaucracy from the perspective of technology critical theory. *National Governance, 7*(25), 26-29.

Mei, J. (2021). Subjective oppression and ethical dilemma in urban digital transformation. *Social Science Abstracts, 19*(9), 37.

Mao, Z. J., Huang, Y. X., & Xu, X. L. (2019). Research on information security risk analysis and countermeasures of smart cities from the perspective of information ecology. *China Administration, 35*(9), 123-129.

Marcuse, R. B. (1988). *Unidirectional people*. (F. Zhang, Trans.). Chongqing: Chongqing Publishing House.

McLean, D. (1995). *Privacy and its invasion*. New York: Praeger Publishers.

Meijer, A. J., Gil-Garcia, J. R., & Bolívar, M. P. R. (2015). Smart city research: Contextual conditions, governance models, and public value assessment. *Social Science Computer Review, 34*(6), 647-656.

Ren, L. L. (2017). Civil law protection of personal information in the age of big data (Ph.D. thesis, University of International Business and Economics, 2017).

Sadowski, J. (2020). *Too smart: How digital capitalism is extracting data, controlling our lives, and taking over the world.* Cambridge Massachusetts, London, England: The MIT Press.

Staddon, J. (2003). Dynamic inference control. In *DMKD03: Proceedings of the 8th ACM SIGMOD Workshop on Research Issues in Data Mining and Knowledge Discovery* (p. 94). San Diego: ACM SIGMOD.

Steinmuller, Lutterbeck, Mallmann, Harbort, Kob, & Schneider. (1972). *Grundfragen des Datenschutzes, Gutachten im Auftrag des Bundesministeriumsdes Inneren (M)*. BT-Drucksache VI3826.

Sun, Y. (2022). Understanding and application of the high penalty system for illegally handling personal information. *Journal of East China University of Political Science and Law, 25*(3), 22-34.

Tang, L. Y. (2021). Legal regulation of privacy computing. *Social Science, 43*(12), 117-125.

Tang, S. S., Zhang, Y. Q., Shan, S. Z., Wang, W., & Zhang, Y. Q. (2020). The development status, situation and policy suggestions of China's new smart city. *E-government, 17*(4), 70-80.

Turkington, R. C., & Allen, A. L. (2002). *Privacy law: Cases and materials* (2nd ed.). Egan: West Group.

Wang, Y. Q. (2022). Defense reasons for infringing the personal privacy of network users in the age of big data. *Journal of Xi'an Petroleum University (Social Science Edition), 31*(3), 84-91.

Wei, X. Y. (2015). Analysis on the risk and avoidance of information consumption in smart city construction. *Library, 43*(3), 75-78.

Westin, A. F. (1968). Privacy and freedom. *Washington and Lee Law Review, 25*(1), 166-170.

Winfried, V. (2018). The GDPR: The emperor's new clothes-on the structural shortcomings of both the old and the new data protection law. Retrieved 21 December 2018 from https://ssrn.com/abstract=3305056

Wu, H. Q. (2014). Connotation and basis of smart city. *Computer CD Software and Application, 17*(19), 10.

Wu, X. L. (2022). Flow cities in the digital age: The rise and governance of new urban form. *Jiangsu Social Sciences, 43*(4), 62-72+242-243.

Xu, K., & Sun, M. X. (2021). Re-clarification of personal confidential information—Starting from the relationship between privacy and personal information. *China Journal of Applied Jurisprudence, 5*(1), 3-19.

Xu, M. (2017). Privacy crisis in the age of big data and its tort law response. *China Legal Science, 34*(1), 130-149.

Zhang, B. X., & Zhou, T. (2016). Can wisdom bring governance—A cold reflection on the construction of smart cities under the new normal. *Journal of Wuhan University (Philosophy and Social Sciences Edition), 69*(1), 21-31.

Zhang, X. B. (2015). From privacy to personal information: Theory and institutional arrangement of interest re-measurement. *China Legal Science, 32*(3), 38-59.

Zhang, X. B. (2019). Personal information collection: Restrictions on the application of the principle of informed consent. *Journal of Comparative Law, 33*(6), 1-20.

Zhen, F., & Qin, X. (2014). Research on the overall framework of smart city top level design. *Modern Urban Research, 29*(10), 7-12.

Zhu, Y. (2011). *General theory of tort liability law: General theory*. Beijing: Law Press.