CHAPTER 2

FACIAL RECOGNITION TECHNOLOGY IN THE DIGITAL ERA

DR IMRANUR RAHMAN
ASSISTANT PROFESSOR
LUCKNOW PUBLIC COLLEGE OF PROFESSIONAL STUDIES
EMAIL: drimranlpcps@gmail.com

MS. SWEETY SINHA
ASSISTANT PROFESSOR
LUCKNOW PUBLIC COLLEGE OF PROFESSIONAL STUDIES

KEYWORDS

DIGITAL RIGHTS FOR PEOPLE, FACIAL RECOGNITION, PERSONAL DATA

ABSTRACT

Facial recognition technology has greatly facilitated our daily lives in the digital age, but it has also increased hazards to private data, property, and privacy, as well as the potential for a degradation of human dignity. When using facial recognition technology, we should exercise caution while keeping in mind the industry's current state of development. We should consider the hazards associated with using this technology, as well as the interests of the public interest, data providers, controllers, users, and regulators. In light of this, we ought to do the following actions: Initially, we ought to mould the "digital rationality" topic by elevating public authority structures and raising individuals' consciousness of their own actions. Second, we should create a realistic normative framework and make the "informed consent" framework for protecting personal information adaptable in light of reality and the current normative system. In conclusion, we ought to establish a multi-governance framework that prioritises accountability and involvement. This can be achieved by reinforcing the duties of regulators and data controllers, encouraging active

public and professional participation, and building an institutional framework that aligns with the "informed consent" framework. These steps are essential to ensuring the security of personal data and are also required to fulfil digital human rights.

2.1 INTRODUCTION

With the advancement of science and technology and the development of society, face recognition has made significant progress in academic research and technological development. In terms of academia, there are more and more research results on face recognition and many of them have entered people's lives. From conventional face feature extraction and high-performance classifier design for features to autonomous learning using convolutional neural networks, the theoretical study of face recognition has progressively advanced. The application of intensity image technology of local binary pattern (LBP), image sequence technology of video training, and 3D information technology of 3D feature extraction has made face information recognition and extraction technologically increasingly feasible and efficient.

Facial recognition technology is pervasive in many facets of productivity and daily life. It is widely used in many different fields, such as control, safety prevention, workplace supervision, and financial behaviour. Face recognition has many advantages over previous identity authentication software, traditional biometric recognition (such as fingerprint, iris, etc.), and other technologies. It is also thought to be very effective and has a great deal of potential for ensuring financial security, public security, and strong interactivity. Other advantages include strong interactivity, no contact, and strong security against theft. However, we are in a new era where technology is rapidly advancing, the overall level of "modernization of the national governance system and governance capacity" is still low, and the difficulty of risk control is increasing.

While facial recognition technology has the potential to enhance governance in certain areas and increase security in these domains, its risks in the risk society could worsen as technology advances, particularly big data technology, which could pose serious risks and hidden hazards to financial security, privacy, information security, and even public security. Thus, facial recognition technology should be "taken seriously" and the possibility of expanding its use to improve people's lives should be recognised as a significant accomplishment of the development of artificial intelligence and big data.

2.2 THEORETICAL AND NORMATIVE IMPLICATIONS OF FACIAL INFORMATION

In daily life, to determine a person's identity, written materials, physical evidence or other evidence are often needed. However, when verifying these evidence materials, most of them need to verify whether it is the person himself by verifying the face. From the perspective of common sense and intuition, the face is one of the most important personal information. However, to what extent this information is related to personal information in the normative sense of our country's civil law, economic law, social law, criminal law, administrative law and even the constitution, it is necessary to observe and demonstrate from the legal level.

2.2.1 NORMATIVE EVOLUTION OF PERSONAL INFORMATION

From the perspective of law, the concept of personal information and its family resemblance have only been created and increasingly concerned in the last half century. This concept has been closely related to privacy since its inception. In the U.S. Privacy Act of 1974, personal information is included in the name of "records maintained on individuals", where "records" refer to "any items, collections or classifications of information about individuals maintained by specialized agencies. This includes, but is not limited to, their educational background, financial transaction records, medical history, criminal or employment records, as well as their names or identification numbers, symbols or other identification features specially assigned to individuals, such as fingerprints or voice prints or photos". As can be seen from the name of the law, personal information or personal records here are subject to privacy.

The protection of personal information is intended to restrict federal agencies and prevent the abuse and dissemination of identifiable personal information by public power in order to protect personal privacy. After that, the Organization for Economic Cooperation and Development issued the "Guidelines on the Protection of Privacy and the Trans-Border Flow of Personal Data" in 1980. The Guidelines include personal information under the term "personal data" in the hope that, in the context of the rapid development of data automation processing technology, it will protect personal information and privacy without excessively affecting international data flows. The legal concept of "personal information" originates from the Privacy Act promulgated in Australia in 1988, which defines it as "information and opinions that can identify or theoretically identify an identity" and emphasizes that whether personal information is true or recorded in material form, it belongs to the personal information stipulated in the Act. Since then, the EU Directive on the Protection of Personal Data Processing and the Free Movement, the UK Data Protection Act, the Japanese and Korean Personal Information Protection Acts, and the Singapore Personal Data Protection Act have all made legal definitions of concepts such as personal data and personal information. The content of personal information provisions in my country's legal documents appeared relatively late. It first appeared in the Several Provisions on Regulating the Order of the Internet Information Service Market (hereinafter referred to as the "Provisions") promulgated by the Ministry of Industry and Information Technology, Regulations emphasizes that without the user's consent, Internet information service providers shall not collect information related to users that can identify users alone or in combination with other information, and refer to this information as "user personal information".

The Notice of the Supreme Court and the Ministry of Public Security on Punishing Criminal Activities Infringing Citizens' Personal Information in accordance with the Law (hereinafter referred to as the Notice) issued, first defined the content of "citizens' personal information", namely "including citizens' names, ages, valid certificate numbers, marital status, work units, education, resumes, home addresses, telephone numbers and other information and data that can identify citizens' personal identities or involve citizens' personal privacy". The Cybersecurity Law promulgated, first made legal provisions for the concept of personal information, namely "various information recorded electronically or otherwise that can identify natural persons' personal identities alone or in combination with other information", personal information of natural persons is protected by law. Any organization or individual who needs to obtain the personal information of others shall obtain it in accordance with the law and ensure the security of the information. It shall not illegally collect, use, process, or transmit the personal information of others, nor shall it illegally buy, sell, provide, or disclose the personal information of others.

2.2.2 NORMATIVE ATTRIBUTES OF FACIAL INFORMATION

It makes reasonable that facial features are important personal information. The face is accompanied by a plethora of labels and attributes that either directly or indirectly communicate the person's personality, behavioural tendencies, rights and obligations, powers and responsibilities, and identity in addition to the individual. From the perspective of norms, whether this information belongs to personal information needs to be further confirmed. From the above-mentioned regulations on personal information, none of them directly lists faces in the definition of personal information. This requires an analysis of face recognition and the normative attributes of faces based on relevant provisions. The above-mentioned relevant regulations all use "identifiability" as the core element to define personal information. In addition, in the "Notice", the extension of personal information is determined by enumeration, and other information and data that can identify the personal identity of citizens or involve the personal privacy of citizens are generally defined by "etc.". Compared with information such as valid ID number, phone number and education level, faces are undoubtedly easier to identify.

Personal information that determines personal identity. In a society of acquaintances, a person's age, ID number or home address may not be known, but their identity can be identified by looking at their face. In a society of strangers, even if the aforementioned information is known, it is still necessary to compare it with the face for verification and confirmation. Therefore, from the perspective of legislative technology, "etc." inherently contains facial information. From the perspective of legal interpretation, "etc." can be interpreted as a matter of course, that is, "etc." certainly contains facial information. Extending this understanding and interpretation to the legal level means that personal information in the Civil Code and other relevant laws, regulations and rules should include faces.

From the definition of the concept of personal information in indian law, facial information belongs to the category of personal biometric information and is an important part of personal information. "The name, date of birth, ID number, personal biometric information, address, telephone number, etc." of a natural person are among the categories of personal information that fall under the purview of Cybersecurity Law. Biometric information is defined as personal data that is produced through certain technical processing that is connected to an individual's anatomical, physiological, or behavioural traits and that can verify that individual's unique identification.

Biometric data is commonly classified into two types: firstly, data derived from an individual's physical or physiological traits, like their fingerprints, iris, face, voice, body odour, etc.; secondly, data derived from their behaviour, like their movement patterns, handwritten signatures, gait analysis, etc. Personal biometric information comprises "personal genes, fingerprints, voiceprints, palm prints, auricles, irises, facial features, etc." according to the pertinent rules in my country. This indicates that facial information should be governed by personal information protection laws since it acknowledges the biometric information properties of facial information at the normative level.

Facial data that is legally protected includes reference templates and digital images. Of these, the reference template is made using the person's picture. Next, the picture information of the facial contour is added after the representative parts of the face are retrieved as features based on their relative position and size. Through this procedure, the face image is converted into a compact and identifiable feature vector that is stored in the background database system for identification and authentication at a later time. The face image used in the photo or video for comparison is known as the digital image. A digital photograph needs to meet two requirements in order to qualify as personal information: first, it needs to feature the person's face clearly and visibly. It is doubtful that the digital image will be considered personal information if it includes scene data that is hazy or distant. The digital image cannot constitute personal information unless the individual in it can be identified, which brings us to our second need. The reference template should also be considered personal information because it includes identifiable face traits and can be linked to a specific person. It is evident that controlling face recognition requires controlling reference templates kept in the automatic recognition system in addition to making targeted changes to the digital picture collection, comparison, storage, and other links.

2.2.3 OVERLAP BETWEEN FACIAL INFORMATION AND PRIVACY

In order to perform facial recognition, the gathered facial images are compared to sample templates stored in the background database. This allows for the exposure of personal privacy to others while also identifying specific individuals in certain instances and tracking their activity trajectory, interpersonal relationships, property status, and other private information. Facial data is significant personal data, but determining whether it may be protected by privacy requires considering the relationship between privacy rights and personal data from both a theoretical and normative perspective.

There are roughly three types of views on the theoretical relationship between personal information and privacy rights, namely, the privacy right inclusion theory, the personal information inclusion theory and the overlapping relationship theory. The privacy right inclusion theory believes that privacy rights have both negative and positive aspects. The former refers to the right to be alone or even "independent" in the traditional sense of private life without being disturbed, and the latter is the right to self-determination of one's own information in the information society.

The subject of privacy rights not only has the right not to be disturbed, but also can decide and use personal information by "doing something". At this time, personal information is an inherent part of privacy, and the purpose of protecting personal information is to defend the right to privacy. The personal information inclusion theory believes that personal information includes privacy. This theory believes that my country's laws confirm that personal information is identifiable, and personal privacy is also identifiable, so it should be included in personal information. The overlapping relationship theory believes that there are both connections and differences between personal information and privacy. The two have the same or similarities in terms of rights subjects and objects, but there are differences in attributes and protection methods. Some scholars also believe that privacy rights mainly involve the balance of interests between different civil subjects, while personal information not only involves the relationship between civil subjects, but also involves national interests, and it is necessary to find a new balance between rights subjects, information practitioners and the state. Some scholars also believe that the traditional privacy protection model can only protect a small part of personal information, and there are more personal information that needs to be protected that cannot be effectively protected by this model under the current background.

The actual demand for personal information protection needs to go beyond the existing privacy protection model. From the perspective of norms and theories, there is an overlapping relationship between personal information, including facial information, and privacy rights. From the provisions of Articles of the Civil Code of my country, at least between private entities, personal information and privacy rights are related and different terms. From the position of the two in the Civil Code, they are interconnected and are both in "Civil Rights", and the subsequent articles all stipulate various specific rights and their remedies. However, which is full of rights, personal information is still not expressed as "personal information rights". Whether it is a right or an interest itself needs further thinking and confirmation.

Therefore, from a normative perspective, personal information and privacy are indeed different and closely related. From a theoretical perspective, although there are three very different views on the relationship between personal information and privacy rights, there are many overlapping areas in the semantic "range" of personal information and privacy rights, and any one of them alone cannot cover the protection and guarantee of the other content. It can be seen that the two are in a complex overlapping relationship. As an important component of personal information, facial information is also in an overlapping relationship with privacy rights. Therefore, the collection and use of facial information may infringe on citizens' privacy rights and personal information.

2.3 RISKS OF FACIAL INFORMATION IN ERA OF DIGITAL HUMAN RIGHTS

2.3.1 THE NEW ERA IS THE ERA OF DIGITAL HUMAN RIGHTS

The new era is an era in which "digital human rights" are increasingly prominent. "Digital human rights" is a brand-new term. It is an emerging human right that is bred and born on the basis of being compatible with the characteristics of the big data era. It has advantages as well as disadvantages. The benefit of digital human rights means that the state should do something to promote and realize digital human rights. In the context of people being unable to avoid and escape from networked life, the Internet is becoming more and more popular. Internet access has become an essential infrastructure for the public, just like transportation, electricity, and tap water. Therefore, digital human rights require the state to do something. The state has the obligation and responsibility to build a good Internet infrastructure, do a good job in the hardware and software engineering construction work involved, and provide various "Internet +" public services that are extended and developed based on these hardware and software. The "right to be alone" in the big data era is a drawback of digital human rights. Even in an era where everyone has access to the Internet and can expand their living space, people still have the right to be free from surveillance and snoopery, to remain anonymous in circumstances unrelated to social and national security, to have their lifestyles unhindered, and to have their rights to privacy protected.

On this basis, without infringing on the interests of the country, society, and others, they can improve their ability to do what they want. Facial information is an important concern of digital human rights, and the risks it faces need to be treated with caution. Facial recognition technology is a technology that emerged with networked life. The positive aspect of digital human rights has contributed to its emergence and increasingly widespread application. At the same time, face is an important personal information. The protection, assurance, and realisation of digital human rights are more clearly demonstrated by the negative aspects of digital human rights, which include the application and collecting of facial information. The new era is an era that intersects with the risk society in time and space. Under the desire to control nature or society more and more perfectly, the risks of the risk society are defined and constructed by professionals who have relevant knowledge and discourse power. However, after creating these risks, they transfer the risks to the public, specific or unspecified groups, so that the risks are shared by the whole society or certain groups, which ultimately leads to the difficulty or even inability to find the subject to bear legal or even moral responsibility after the interests or rights of these groups are infringed. Therefore, in the digital risk society, face information faces huge risks.

2.3.2 PRIVACY THREATS AND PROPERTY RISKS FACED BY FACE INFORMATION

Faces have particular meaning for individuals in a variety of social contexts and cultural traditions. In the risk society, dangers and threats to societal, national, and private security, as well as risks to personal privacy and safety, may arise from the widespread collection of face data into big data. The creation and use of big data on facial information may pose a risk or threat. One could argue that the acquisition of face data violates people's right to privacy. Although the face does not directly convey privacy, it does contain significant personal information that is linked to privacy. From the definition of privacy, whether it is defined as "personal private affairs that are unwilling to tell others or make public", or the right to resist public power search and arrest, or the "semi-constitutional" freedom related to freedom of speech, the face can hardly be called privacy.

Otherwise, every day in daily life, everyone goes out with privacy on their faces, and people's appearance is equivalent to their privacy being actively leaked. Although the face itself is not private, it undoubtedly carries important personal information. If "identifiability" is used as the standard for personal information and its protection, the face is even the most representative personal information. If we follow the traditional standpoint and view, and define privacy as the secrets of a person's private life, including private information, private activities and private space, then even if the face itself does not belong to personal privacy, the personal information it carries and the time and space where it appears may constitute privacy. When facing problems in the real world, we need a pair of "thinking glasses" to discover the truth behind the complex phenomena in the world around us with keen insight.

The processing method of big data is similar to providing a pair of special glasses to the data processor, so that it can discover the true face and even thoughts of a person behind the fragmented and chaotic personal information, and form a full-scale insight into a certain individual. As a result, big data technology has created a "big data glasses" that can penetrate the information fog and fully control personal information.On the other hand, the collection and application of facial information may bring unpredictable risks to personal and property safety, and even threaten public interests and national security. Regarding the complex and fragmented information in life, some philosophers have keenly observed that "some people hear only noise, while others hear melody from it". The same seems to be true for personal information. Fragmented personal information is equivalent to noise, but "interested people" integrate personal information through technical means, just like arranging and combining the rhythms in noise to form a melody. Those faces that are placed under different cameras in a scattered or even scattered form in life may be just an ordinary face that has nothing to do with oneself to someone who sees this face alone, just like a meaningless noise or a piece of noise heard accidentally. But after being integrated with big data, these "noises" may become "melodies".

Through mining, a lot of information, secrets and privacy that individuals do not want to be known can be obtained, and even important information related to social stability and national security can be obtained. For individuals, face recognition technology is applied to many bank or online financial product payment behaviours, community access control and even the opening of private house doors. After these facial information is obtained by facial recognition equipment manufacturers and community property agencies, it is difficult to ensure that it will not be leaked and abused. At the same time, the network security facilities of these institutions, the network security awareness and technology of relevant personnel, etc., are also difficult to ensure that facial information is in a safe state for a long time. When facial data is gathered and utilised by unaffiliated parties, people may be exposed to unanticipated threats. Over-collection of face data could be detrimental to both national security and social order. Of course, the risk here only means the possibility of privacy or property infringement, and it does not mean that it will definitely happen.

Enterprises or institutions that use facial recognition technology are also taking some measures to prevent risks. In practice, there have been cases where deception has been discovered through liveness detection in facial recognition, such as the discovery of fraud in a certain online loan APP through face recognition liveness detection, and thus the discovery of criminal behaviour of impersonating the detector. At the same time, research on cracking face recognition has been ongoing, and many advances have also made people maintain a sufficiently cautious attitude towards the security of face recognition technology. Research results show that adversarial stickers can deceive face recognition lenses 49.6% of the time. Researchers from Huawei Moscow Research Institute and Moscow State University have created a unique paper pattern that may produce adversarial assault images on paper that mimic three-dimensional visuals, fooling artificial intelligence. The face recognition system won't be able to identify the person's true image if this paper is applied to the head. Even for live tests, ideas and methods for cracking through 3D face modelling have been generated. All of these fully show that various face recognition deceptive technologies and means are constantly challenging the certification capabilities of enterprises, social organizations and even countries, and face recognition technology has considerable risks in the application process.

2.3.3 THE RISK OF DIGNITY DEGRADATION FACED BY FACE INFORMATION

Sometimes, the collection of face information does not directly infringe on personal privacy, but it may directly infringe on human dignity and devalue the value core of all rights enjoyed by people. Human dignity is a value cherished and pursued by mankind. People not only care about their own safety, but also people protect themselves, pursue wealth because they care about improving their material living conditions, and have an instinctive and subtle sense of their own value, and the devaluation of this is no less than the damage to their bodies and property. In many cases, people's pursuit of this value exceeds their lives and property, which is why there are behaviours such as "regarding unjust wealth as floating clouds" and "sacrificing one's life for justice". Therefore, "in the name of human beings, there is a kind of dignity that is felt". The core value of human dignity has been widely respected and affirmed worldwide and is reflected in many legal norms. My country has also made such provisions at the level of private law and public law. The rapid development of face recognition technology has continuously expanded the space and scope of its application, and in the process has rapidly reduced the cost of equipment operation and use. As the cost decreases, the sales of face recognition equipment will increase and may be applied on a larger scale. While enjoying the convenience brought by the advanced technology of face recognition, we are also facing the problem that some basic legal values may be eroded. In some cases, the application of face recognition directly involves the issue of human dignity.

The meaning and function of "face" in social culture make it inherently contain human dignity. Compared with other types of personal information, we should pay attention to the cultural attributes of "face" itself and its psychological impact on individuals. Punching in, fingerprint sign-in (at this time we will not consider the issue of personal information protection in fingerprints), and face sign-in are all ways of signing in, but face sign-in is undoubtedly more likely to produce a psychological sense of being offended. Face has a special connotation in the cultural landscape. It is not only the arrangement and integration of a person's facial features, but also has rich social and cultural functions, with obvious normativeness and radiation, and is closely related to "a series of normative behaviors shown in a certain social situation", including "the psychology and behaviour of identity shown after impression decoration". Face also carries profound social significance in various cultural systems in the world. The face not only means a human organ, but also reflects a certain emotion, character and personality." Face" is not only a "face" in the physiological sense, but also a "face" in the psychological sense. It contains some non-verbal information that can be used to judge the subject's emotions, opinions, and attitudes. It is also associated with "respect" at the abstract cognitive level, which means the respect that individuals, families, etc. get from others. Therefore, "face" is not only a part of the body, it also represents or is equivalent to the whole person, including the spirit, and forms a link relationship with a stable personality, representing the personality in an explicit or implicit way.

In life practice, many facial recognition devices are installed without the informed consent of the parties, including not being informed in the true sense due to insufficient cognitive ability or information asymmetry of the parties, and not being able to agree or object from the heart after being informed. Specifically, there are the following ways: First, some people do not know what facial recognition means to individuals, and just think that "it's just a face scan, and they don't lose anything"; second, some people do not know whether their information storage is safe after being "scanned", and they don't know knowing what organizations will use their facial information for what purposes in the future, and whether these purposes are harmful to their economic interests and personal dignity; third, some people know or can foresee that being "face scanned" may have adverse consequences for themselves, or they do not understand the consequences but think that "face scanning" itself is an offense to themselves, but because they are employees of a certain unit or community members, they are embarrassed to oppose or worry that opposing will alienate themselves from their group; fourth, the parties know the possible risks of facial recognition and oppose it, but under direct pressure, such as losing their jobs or receiving salary cuts, reduced treatment or even threats of violence, they have to accept facial recognition. In either case, this is a violation of the principle of informed consent, and even an infringement of the free will and personal dignity of the parties. Some people may think that face scanning without informed consent is an offense to human dignity, then face scanning after informed consent does not offend human dignity.

This view emphasizes the importance of autonomy of will, and believes that informed consent reflects that the parties set rights and obligations for themselves through their true intentions, so that the use of personal information or face scanning has a legitimate basis. However, this cognition may overlook the word "real" in "real meaning". First, people may only "know" rather than be informed in the true sense. Limited by people's ability to understand information and their own judgment of things, as well as the influence of the external environment, people may often know the existence of something related to themselves, but do not know the real interests of this event, so they may "agree" without understanding or consideration. Secondly, even if they are truly "informed", they may have to "agree". This kind of consent, in a formal sense, meets the requirements of current laws and regulations, but it may not truly reflect their free will, so it is difficult to be called true consent.

Sometimes, people are constrained by coercion and have to agree, just as some forced sales are legal in form. Sometimes people may not face direct or indirect threats of force, and clearly know what consequences their consent will bring, but they have to agree due to the situation and reality, just like a worker who urgently needs to support his family has to sign a labour contract that is very harsh and poorly paid. At this point, he may know where his best interests lie, but he is constrained by reality and is forced to agree. It is conceivable that when facing employment or similar pressure, it is difficult for a person to refuse institutional arrangements such as face-scanning sign-in and face-scanning salary. "Face" is a symbol of personal social identity and a pass for interpersonal communication and building trust. But in the era of face scanning, the face is automatically captured by cameras and other devices to generate digital images to identify, authenticate or verify specific individuals, becoming a tool for identification and being identified.

As a result, the "face scanning" behaviour without the true informed consent of the parties becomes an act of power and obedience—regardless of whether this power is state power or social power. The personality factors behind the face and the values such as trust and dignity it carries are diluted, captured and obscured by technology. Computer technology and new measurement methods have successfully turned a person with an independent personality into a series of numbers and codes, and transformed a living person into rows of data. At this time, what is identified is the face, what is obtained is data, and what is lost or devalued is the subjectivity and dignity of the person.

2.4 MEASUREMENT IN THE APPLICATION OF FACE RECOGNITION TECHNOLOGY

Since face recognition technology involves important personal information when applied and directly affects the realization of digital human rights, it should be used with caution. In order to meet people's wants for a better living and to modernise the national governing system and governance capability, cautious usage first means "use" and embracing scientific and technological advancements with positivity. Careful use highlights the necessity to approach it cautiously, particularly in a contemporary world full of emerging threats. We shouldn't let the industry that uses the technology "grow wildly" or let the technology itself continue to advance unchecked. Because it is difficult to obtain appropriate relief and even more so to fully restore the original state if the face information that is trapped by the "wild" industry is lost or misused.

If mobile phone numbers, home addresses and even names can be changed to avoid greater infringement of personal interests and rights, then since faces cannot be changed, the damage caused by the loss or abuse of face information may be long-term or even permanent, and the difficulty of remediation will increase exponentially. Therefore, scientific and serious evaluation is needed when applying face recognition technology, and different parties such as information owners, enterprises, and governments, risks, costs and benefits of the whole body are weighed.

2.4.1 THE NECESSITY OF WEIGHING THE BENEFITS OF FACE RECOGNITION TECHNOLOGY APPLICATIONS

The term "benefit weighing" is often used in judicial practice. However, when regulating certain behaviors, it is also possible to weigh the relevant risks, costs and benefits of different subjects through legislation to formulate more reasonable rules. When governing the application of face recognition technology, corresponding rules can be formulated on the basis of interest weighing to achieve a balance of rights and obligations among different subjects.

In a risk society, it is necessary to weigh the risks and benefits brought by new technologies. The risks brought by new technologies and the systems that accompany them are a kind of "man-made risks", which may surpass natural risks and become the main content of risk society. Some technologies and institutional arrangements are originally intended to make our lives more certain and predictable. In the early stages of their operation, they did achieve their intended purpose, but in the end they may bring results contrary to their original intentions. Compared with the external risks brought by the immutability and fixity of tradition or nature, this risk that accompanies the development of science and technology and the advancement of knowledge is a manufactured risk, and past life experience, technical means and organizational systems are no longer sufficient for us to prevent, avoid and respond to the threat of new social risks.

The application of face recognition technology brings such a risk. It can provide convenient payment methods, more reliable identity recognition than ever before, more orderly traffic order and safer social environment, which can improve our quality of life in an all-round and holistic way. At the same time, the risks it brings are also reflected in the aforementioned areas. The impact of these risks on people's lives is unpredictable and sometimes may be so huge that even Microsoft, which is happy to collect personal information and obtain huge profits from it, requires increased supervision of biometric privacy to respond to or avoid such risks.

Therefore, when evaluating face recognition technology, we must place ourselves in the context of risk society and its accompanying "artificial risks", measure the risks and benefits faced by different subjects in face recognition applications, and reasonably allocate the rights and obligations between relevant subjects.

2.4.2 CONTENTS OF INTEREST MEASUREMENT IN FACE RECOGNITION APPLICATIONS

When evaluating the application of a face recognition technology, its costs and benefits should be evaluated and the costs and benefits of the parties involved should be reasonably distributed. The author does not intend to give the evaluation indicators and system in this article, because this is an extremely complex task that requires a strong team to complete this task through long-term efforts. If we agree that the essence of law is a kind of "plan", then at least the following factors should be considered in the evaluation: subject, cost, and risk, benefit, and consider how to fairly share costs, risks and benefits among different subjects. In addition, when discussing the relationship between rational behaviour and institutional constraints, the inherent political and social factors in social life cannot be ignored. For example, different countries are influenced and constrained by historical culture and social systems, and their people have different preferences for different types of values.

- **Measurement of different subjects-** The risk-benefit assessment of the application of face recognition technology should consider the two major subjects of information collectors and information collected, as well as representatives, society and country of public interest. Information collectors include individuals, enterprises, governments and other entities that apply this technology, as well as enterprises that develop this application technology. These entities can obtain facial information from the aforementioned entities after selling technology and services. Information collectors are individuals, including not only employees who are required to perform facial recognition in the unit, but also passengers in airports, subway stations, bus stations and other places, as well as customers shopping in shopping malls, administrative counterparts handling affairs in public service agencies, patients visiting hospitals and even pedestrians on the street. Of course, there may be overlapping identities among these people.
- **Measurement of risks and costs-** It should be emphasized that cost and risk are one and the same. In addition to actual expenditures or losses, the size of the risk and its probability of occurrence are also ways to determine the cost, and even the risk itself constitutes an important cost. Of course, this cost includes both the loss of specific material wealth and the emotional and spiritual damage caused by the loss of rights, as well as the resulting devaluation of human dignity. Correspondingly, benefits also have objective and subjective aspects. If material wealth is regarded as an objective benefit, then emotional and spiritual benefits can be called subjective benefits. Subjective interests are subjective and difficult to identify. Different living spaces, lifestyles, and even individual life experiences may affect the perception and judgment of such interests. For example, people in rural and urban areas, perpetrators and victims of illegal and criminal acts may have different perceptions of interests in behaviors involving privacy, expression, "face", etc., and have different feelings about whether face scanning infringes on their subjective interests and to what extent.

In addition, there is still room for further research in terms of how to measure subjective interests and objective interests. For example, when people face unfair distribution plans, the anterior insula and dorsolateral prefrontal cortex are significantly activated. The anterior insula is responsible for emotional processing and is related to emotions of disgust and anger, while the dorsolateral prefrontal cortex is responsible for the cognitive system's inhibition of emotions. This shows that at this time, people's pursuit of subjective interests such as fairness and sense of fairness exceeds economic interests. Even if there is no effective method and mechanism for the universal calculation and measurement of subjective and objective interests in the current context, at least these two factors should be considered in the evaluation. For risks that have not yet caused damage or the extent of which is difficult to predict, there are already real cases that regulate them to protect the rights and interests of risk subjects. For example, in 2008, the State of Illinois enacted the Biometric Information Privacy Act (BIPA), which stipulates the rules for the collection, storage and processing of data, including data generated by retinal or iris scans, fingerprints, voiceprints, hand or face geometry scans, and other biometric information or biometric data from the public. Consumers can sue infringers for improper storage or use of their information, or unauthorized disclosure, regardless of whether substantial damage is caused.

- **Measurement of public order and safety-** In addition, there is a part of the benefits that are reflected in public order and public safety. Although the benefits of such public products are difficult to price, they should at least be considered when formulating public policies. Public order and public safety include both online and offline areas. The online area refers to network security. According to Cybersecurity Law, "Network security refers to taking necessary measures to prevent attacks, intrusions, interference, destruction and illegal use of the network and accidents, so that the network is in a stable and reliable state of operation, and to ensure the safety of network data.

This means that network security involves network product and service security, network operation security, network data security, network information security and other major aspects. Network security is a basic public good required by both the state and citizens. Because, "citizens hope that their government can protect them from mutual harm on the Internet and prevent damage from abroad. Companies need a legal environment that can guarantee the stability of the network and enable the prosperity of Internet business." The offline field refers to the security of real life outside the Internet, which includes good public security, safe transportation, orderly social life and predictable behaviour patterns and results. Although this part of the benefits is not for specific individuals, it is enjoyed by all social entities. It can not only protect the real security of each individual, but also provide guarantees for its long-term development, so it is an indispensable public interest.

2.5 GOVERNANCE PATH FOR THE APPLICATION OF FACE RECOGNITION TECHNOLOGY

Ministry of Industry and Information Technology officially issued 5G commercial licenses to Telecom, and Broadcasting Corporation. This means that my country will officially enter the 5G commercial use. As we get closer to the 5G era, the Internet of Everything brings unlimited possibilities for the emergence and development of new technologies, new applications, and new businesses. There are also various possibilities for the application scope, methods, and methods of face recognition technology. But the more so, the more we should pay attention to the risks brought by face recognition. In order to assure the realisation of digital human rights in the new era, we should respect and safeguard human dignity while encouraging the use of new technologies and the creation of new enterprises.

2.5.1 SHAPING A SUBJECT WITH "DIGITAL RATIONALITY"

Human rationality is a complex academic topic. In the current era of big data where information flows extremely rapidly, and in the context where everything, including humans, is a link in the data chain, we need to re-understand human rationality, and our understanding of humans needs to shift from focusing on individuals (and groups composed of individuals) to focusing on "relationships", interactions and mobility, and this interaction and mobility should also be "warm, breath, and emotions". Therefore, "we can no longer just regard ourselves as individuals who make prudent decisions, but must consider the dynamic social effects that affect personal decisions and drive economic bubbles, political revolutions and the Internet economy." In the context of the era of the Internet of Everything, we should shift from focusing on the economic rationality or social rationality of independent individuals to focusing on the relational rationality of exchange or interdependence between people. This rationality can be called "digital rationality". The cultivation of "digital rationality" requires not only people's own continuous learning and updating, but also the actions of public power agencies and the state.

2.5.2 SELF-CULTIVATION OF THE "DIGITAL RATIONAL" SUBJECT

The subject should first have Internet thinking. This means that the subject should view the relationship between individuals and online goods and service providers, the relationship between the use of personal information and industrial development based on relational rationality during the interaction process, understand the costs and risks faced by themselves for the services they enjoy, and understand the basic rights and obligations of themselves and related subjects. From the beginning of the Internet to the present, whether in advertisements promoted by various media including self-media, or in the practice of personal use of the Internet, "free" and "sharing" are a consensus judgment, it seems that people can use certain websites, software and apps for free without paying for them. In fact, as long as there is a connection with such service providers on the Internet, virtual or physical production has occurred.

Various platform companies "collect more data through various means, predict and shape economic consumption habits through sophisticated algorithms, provide accurate personalized services, control transaction and production channels, and capture more consumer surplus and producer surplus." Therefore, "digital rational" subjects should not regard the enjoyment of services as cost-free consumption or free riding, but should understand that providing personal information including face recognition is the price of paying for these services, and this price not only provides the productivity needed by Internet companies and provides direct impetus for the development of the Internet industry, but also brings various potential risks to their future lives. He should also realize that when enjoying seemingly free Internet services, he should understand his own and the service providers' respective rights and obligations, and use network services on the basis of true informed consent, rather than completely ignoring the informed consent form or ignoring it because it is too complicated. In addition, he should also conduct activities on the Internet based on the law and public order and good morals, and at the same time be aware that the network authorities and relevant agencies have the power and responsibility to govern the Internet, including the power to effectively supervise to avoid the abuse of personal information.

The "digital rational" subject should also continuously improve its rational social cognitive ability and eliminate cognitive bias. Improving rational social cognitive ability is a process of continuous learning and acquisition. Just as negative emotions and cognitions such as anxiety and helplessness can be acquired, optimism and rationality can also become the ability of individuals to recognize society through acquisition. On this basis, even disciplines such as "positive psychology" have been created and such research has received high social evaluation. Similarly, just as people can choose to treat the world with a pessimistic or optimistic attitude, people can also choose to treat social problems and social phenomena with a rational attitude, eliminate cognitive bias, and rationally treat the positive and negative effects of face recognition In this way, he can neither indulge in the convenience and efficiency brought by the Internet, nor can he carefully evaluate the privacy risks, security risks and financial risks it brings.

2.5.3 THE PROMOTION OF "DIGITAL RATIONALITY" BY PUBLIC AUTHORITIES

The improvement of rational social cognitive ability does not only come from the acquisition and improvement of citizens' self-cultivation, but also requires public authorities to do something and not do something through warm and cold actions and institutional arrangements. First, public authorities should treat personal information, including faces, with a responsible attitude, which includes taking strict security measures to prevent the leakage of collected information and making the public aware of the risks of collecting and applying such information. They should not only promote the convenience of facial recognition or installation of equipment for public safety and management, but also intentionally or unintentionally ignore the disclosure of relevant information, so that the public cannot know, understand and understand the potential risks and negative impacts of these measures on themselves. Secondly, the state should implement laws and regulations more effectively to reduce the public's insecurity about the leakage of personal information. Through a strong crackdown on online fraud and telephone fraud, and effective supervision of online platforms and other public authorities and enterprises and institutions that hold personal information, people can truly enjoy the freedom from the fear of personal information leakage.

Thirdly, do a good job in public opinion guidance and psychological intervention, and reasonably guide and optimize social cognition. When people are continuously or long-term exposed to a certain stimulus, they will have a dull reaction to this stimulus, and lead to long-term changes in cognition, emotions and behaviors, and even form a personality with certain negative characteristics. Based on this personality and behaviour pattern, the "subconscious knowledge reserve" obtained from the accumulation of negative experiences may "naturally" form some negative intuitive reactions. Therefore, public authorities should do a good job in guiding public opinion to avoid the public from being desensitized to certain negative behaviors. In terms of face recognition or personal information, it is necessary to avoid the formation of "desensitization to infringement" and avoid people from forming this has become an implicit social perception that people will not seek redress for their rights being infringed.

2.5.4 CONSTRUCTING A REASONABLE REGULATORY SYSTEM

For personal information protection, my country has already had a number of relevant laws, regulations, rules and judicial interpretations that directly or indirectly provide for it. This has formed a complete set of personal information protection regulatory systems from constitutional administrative law to civil law, economic law, social law and even criminal law. The law should reflect the respect, protection and guarantee of citizens' interests and rights, the strengthening and promotion of public interests, and the emphasis and guidance of the development of emerging industries in terms of legislative concepts and principles. At the same time, it should be able to coordinate with the current constitution and laws to maintain the coherence of the legal system.

2.6 VARIOUS SYSTEMS OF GOVERNANCE BASED ON ACCOUNTABILITY AND INVOLVEMENT

For the use and protection of personal information, including faces, a multiple governance mechanism should be formed to strengthen the responsibilities of data regulators, controllers and users, and distribute the interests, rights and responsibilities between data providers, controllers and regulators through this mechanism. This mechanism is based on the existing institutional framework, forms public opinion through multi-subject participation and interaction, forms a practical implementation method, and realizes the purpose and function of industrialization of personal information use and digital human rights protection.

2.6.1 RESPONSIBILITIES OF DATA REGULATORS AND CONTROLLERS

This mechanism emphasizes the responsibilities of regulators and data controllers. This is because, from the perspective of cost control, it will cost a lot to let all users involved in data production decide whether to agree to the collection of personal data based on informed consent. Due to people's understanding ability, emotional influence, information asymmetry and cognitive bias, although it is necessary to improve people's digital rationality, it is not realistic to cultivate everyone into a completely rational subject, and it is also a job with very low marginal benefits. Therefore, while cultivating public rationality, it is more cost-effective and effective to focus on how to assign obligations to data supervisors and controllers, which is more conducive to effective data governance and the protection of citizens' personal information and digital human rights

2.6.2 EFFECTIVE PARTICIPATION OF THE PUBLIC AND PROFESSIONALS

This mechanism emphasizes the openness, democracy and inclusiveness of rule-making and decision-making, and emphasizes the effective participation of professionals. Even if we only talk about the present rather than the future 5G era, the use of personal information and its desensitized sales are still big business. This is a large undertaking that concerns the information interests and rights of almost everyone, public interests and even national security. It must be governed in an open and democratic manner. Openness means avoiding "black box operations" and adopting methods such as publishing agendas, publishing records, and allowing audiences to listen, and combining these methods with the Internet so that people can understand and know the handling of such issues, and let the rules and decisions that concern the interests and rights of all people be known. This is the premise and foundation for subsequent democratic participation.

The democracy mentioned here includes both the "common core" of traditional democracy - citizen participation, and the characteristics of democracy itself in the digital age - the voices should be heard rather than drowned in the ocean of information overload. In the Internet age, it is often a very small number of websites that occupy the vast majority of links and visits, and more websites and the information they carry are difficult to see. Search engines play an important guiding role in link and traffic distribution. Some people directly call this unequal order "Googlearchy". At this time, in the Internet era, information overload and information shortage (the public cannot see the information they want to see or should see) coexist. We need better filtering tools to filter out junk information to obtain effective information.

At the same time, the governance of personal information and data requires the participation of professionals. Although everyone can express their own views on personal information issues, the importance of this information and data, the technical tools needed to process them, and the consequences they produce require the joint participation of different professional groups including the Internet, big data, industrialists, and legal professionals. Listening to various voices from different industries can allow us to understand and recognize the complexity of the problem while avoiding the "crowding and stupidity" of single industry experts in discussions and decision-making.

2.6.3 IMPROVE THE COMPATIBILITY OF "FLEXIBLE" INFORMED CONSENT

The "flexible" informed consent model has a formal adherence to classics and traditions, but through text processing and corresponding institutional arrangements, it can be compatible with or even integrate certain needs of the "scenario theory" and even the "social control" model. Therefore, multiple governance mechanisms can be realized in the "flexible" informed consent model. Specifically: First, take into account and emphasize the responsibilities of regulators and controllers. For example, it stipulates the supervision system and supervision system for personal information protection, emphasizes the state's obligation to protect personal information, stipulates the social responsibility of information providers, the social obligations of industry organizations and personal information protection organizations to protect personal information based on public welfare, and forms a socialized service system for personal information protection around these subjects. Secondly, while maintaining respect for individual rationality, it also considers the problem of insufficient rationality of people. By making informed consent "flexible", it provides space for the parties to reconfigure the rights and obligations between individuals, the state and information providers through contracts. In the case of information asymmetry, insufficient personal cognitive ability or being constrained by the scene and having no time to be informed in detail, people often "have to" be informed and agree.

The drafters are aware of this possibility and make a certain degree of remedy, requiring "information providers and government departments should use clear and easy-to-understand terms to fully, accurately and promptly inform the information subject of the purpose, method, scope and other related matters of their personal information processing", while excluding "presumed consent" and stipulating that "the consent of the information subject should be made by clear intention or behaviour" and "the silence of the information subject without refusal shall not be deemed as consent". Finally, improve the compatibility with scenario theory. The scenario theory focuses on "taking differentiated safeguard measures according to specific scenarios, changing static compliance before information processing to dynamic risk control during information use".

By stipulating the exception of "implied consent is not deemed as consent", clause emphasizes that when "there are other provisions in laws, administrative regulations or other agreements with the information subject", the consent of the subject can be presumed. This helps various stakeholders to form diversified and situational rights and interests arrangements on issues such as the collection, storage, use, transaction and benefit distribution of personal information. This also helps to form a personal information system centred on contracts and transaction mechanisms, which can more flexibly take into account the different characteristics of personal information issues in different time and space contexts, and enable regulatory authorities to simultaneously leverage the centralized review of standard contracts and the decentralized adjudication of contract disputes to make these systems more effectively implemented.

2.7 IMPLEMENTATION METHODS OF MULTIPLE GOVERNANCE MECHANISMS

Multiple governance mechanisms based on responsibilities and subject participation can be achieved through institutional settings, institutional arrangements, and normative docking. First, set up a dedicated data protection agency. In the field of network information security, my country has formed a unified leadership system led by Cyberspace Security. However, at the level of specific working mechanisms, there is still a lack of unified planning, deployment, and coordination, which makes it difficult to implement many established principled norms and the lack of compliance guidance for regulatory objects. In order to strengthen the unity of power and responsibility in the supervision of this field and ensure the integrity of relevant policy thinking and practice, we can refer to the idea of establishing a special data protection agency in the European Union and European countries, and set up or select a department under the unified leadership of the central government to coordinate policy formulation and law enforcement coordination in the field of personal information protection.

Secondly, formulate multiple systems to regulate multiple subjects and realize three-dimensional governance from public power organs to private institutions, from laws to social norms, and from transactions to insurance mechanisms. Personal information, including faces, is authentication information for identifying and confirming personal identity. The power of face scanning and other identification and authentication of personal information is a security authentication power. Public institutions and private institutions have different qualifications and powers when authenticating personal information, and their face scanning behaviour should also have different normative basis or contractual agreement accordingly, otherwise it will blur the boundaries between public services and private services, forming a confusion of different identities and powers.

Therefore, in addition to determining rights at the legal level, the focus of the future construction of personal information protection system should also promote the formation of social norms and conduct more detailed contract and transaction mechanism design. Through social norms, the data behaviour of the government and commercial entities is restricted, and through contracts and transaction mechanisms, various stakeholders are encouraged to form diversified and situational rights and interests arrangements on issues such as personal information collection, storage, use, transaction and benefit distribution.

In addition, the research and design of personal information damage insurance mechanisms should be strengthened, and the insurance mechanism should be fully utilized to make up for the shortcomings of civil litigation in risk management and loss repair. Finally, the integration of different departmental laws and regulations should be achieved to protect personal information in an integrated manner. In order to effectively protect personal information, in addition to reasonably allocating rights in the civil field, respecting market innovation in the use of personal information and effectively regulating it, it should also be effectively connected with the relevant rules of administrative law and criminal law, and severely punishing and maintaining a high-pressure situation for those behaviours that break the moral bottom line and infringe on personal information, such as the collection, sale and even fraud of personal sensitive information and information of minors.

2.8 CONCLUSION

In a time when face recognition technology is extensively employed, we need to be mindful of the preservation and upholding of digital human rights in addition to keeping an open and welcoming mindset regarding the use of new technologies and the growth of new companies. Facial information is an essential component of personal information, a fundamental right that should be taken into consideration when discussing digital human rights, and people's unique biometric information—at least temporarily. "Use it with caution" is the advice. When governing the application of facial recognition technology, we must reasonably allocate risks and benefits in the context of the big data era. We must reasonably divide the rights, obligations and responsibilities between the people whose biometric information is collected, the users and controllers of biometric information, and the regulators, and strengthen the responsibilities of data supervisors, controllers and users. Based on this concept and principle, we can make a reasonable allocation of risks and benefits in the context of the big data era.

First, we should take measures with an open and inclusive mindset to shape the digital rationality of digital human rights subjects, so that they can remain rational about the convenience and surprises brought by new technologies and have a basic understanding of the risks and benefits that come with them. Secondly, formulate a personal information protection law with a reasonable structure and content and build a series of supporting and operational multiple normative systems. Finally, create a set of social norms and several governance systems based on accountability and participation using an open, democratic, and professional approach. The modernisation of national and social governance systems and governance capabilities can be enhanced in a multifaceted and multilevel manner by forming the digital rational subjects of the new era, enhancing the legal normative framework, and implementing different governance mechanisms.

2.9 REFERENCE

- Zhao Jinsong: "Cool Upgrade: "Face Scanning" Technology is Here!", published in "Nanfang Morning Post" on October 25, 2018, page A108.
- Chen Yaodan and Wang Lianming: "Face Recognition Method Based on Convolutional Neural Network", Journal of Northeast Normal University (Natural Science Edition), No. 2, 2016, pp. 70-76.
- Prasad K. K. , P. S. Aithal, A Conceptual Study on User Identification and Verification Process Using Face Recognition Techniques,
- International Journal of Applied Engineering and Management Letters (IJAEML), 6-17 (2017).

- Jing Chenkai et al.: "A Review of Face Recognition Technology Based on Deep Convolutional Neural Network", Computer Applications and Software, No. 1, 2018, pp. 223-231.
- Ulrich Beck: "Risk Society", translated by He Bowen, Yilin Press, 2004 edition, pp. 15-47.
- Zhang Xinbao: "From Privacy to Personal Information: Theory and Institutional Arrangement of Re-weighing Interests", China Legal Science, No. 3, 2015, pp. 38-59.
- Xie Yuanyang: "The Value of Personal Information from the Perspective of Information Theory - A Review of the Privacy Protection Model", Tsinghua Law Review, No. 3, 2015, pp. 94-110.
- Zhang Wenxian: "The concept of 'digital human rights' has a solid legal basis, practical needs and great significance - 'No digital, no human rights'", Beijing Daily, September 2, 2019, p. 15.
- Jiang Jianguo: "Networked survival, the spread of online loneliness and psychological crisis", Exploration and Debate, No. 10, 2013, pp. 81-85.
- India, Amartya Sen: Development as Freedom, translated by Ren Ze and Yu Zhen, China Renmin University Press, 2002, p. 13.
- Germany, Ulrich Beck: Risk Society, translated by He Bowen, Yilin Press, 2004, p. 20.
- Modern Chinese Dictionary (Fifth Edition), Commercial Press, 2005, p. 1629.
- Ken Gormley, One Hundred Years of Privacy, Wisconsin Law Review, 1335-1442 (1992).
- Yang Lixin: Privacy, Inviolable, People's Daily, September 8, 1999, p. 11.
- Alister McGrath: The Surprise of Meaning: Science, Faith, and How to Understand the Meaning of Things, translated by Sun Weikun, Sanlian Bookstore, 2014, p. 19
- Yang Weiyue et al.: "Multi-pose face synthesis method for 3D modeling", published in "Chinese Science and Technology Papers" No. 14, 2018, pp. 1573-1577.
- Guo Chunzhen, On the Relationship between Two Human Rights Preferences and the Positive Aspects of Human Rights in China, Legal Review, No. 2, 2012, pp. 11-17.
- He Xi and Zhu Ying: "Social Cognitive Neuroscience Research on the Self", Journal of Peking University (Natural Science Edition), No. 6, 2010, pp. 1021-1024.

- Lang Sheng: "Explanation on the Draft Cybersecurity Law of the People's Republic of China", China Communications Security, No. 8, 2015, pp. 52-55; Yang Heqing, ed.: Interpretation of the Cybersecurity Law of the People's Republic of China, China Legal Publishing House, 2017, pp. 191-194.
- Jack Goldsmith, Tim Wu, Who controls the internet? Illusions of a borderless world. New York, Oxford University Press, 2006, p. VIII.
- Xinhuanet: "The Ministry of Industry and Information Technology will issue 5G commercial licenses in the near future", http://www.xinhuanet.com/2019-06/03/c_1124577284.htm, accessed on November 5, 2019.
- Duan Yongchao: "Measurement or Perception", in Alex Pentland: Smart Society: Big Data and Social Physics, translated by Wang Xiaofan and Wang Rong, Zhejiang People's Publishing House, 2015, preface, page XV.
- Alex Pentland: Smart Society: Big Data and Social Physics, translated by Wang Xiaofan and Wang Rong, Zhejiang People's Publishing House, 2015, page 6.
- He Lai: "Relational Rationality and the Real "Community", in Chinese Social Sciences, No. 6, 2015, pp. 22-44.
- Cavoukian A, Taylor Sand Abrams M E., Privacy by Design: Essential for Organizational Accountability and Strong Business Practices, 3(2), Identity in the Information Society, 405-413 (2010).
- US, Michael Fettik and David C. Thompson: "Reputation Economy: The Value of Personal Information and Business Transformation in the Big Data Era", translated by Wang Zhen, CITIC Press, 2016, pp. 9-17.
- Guo Qiuyong: "Three Major Theories of Contemporary Democracy", Xinxing Press, 2006 edition, pp. 9-11.
- US, Matthew Hindman: "The Myth of Digital Democracy", translated by Tang Jie, China University of Political Science and Law Press, 2016 edition, p. 71.
- Adrian Vermeule, The Constitution of Risk, New York, Cambridge University Press, 2014, p. 164-165. Quoted from Zheng Ge: "Towards a Constitution of Life-How the Law Responds to the Risks in the Application of Gene Editing Technology", "Legal and Commercial Research", No. 2, 2019, p. 5.
- Zhang Xinbao, Ge Xin: "Personal Information Protection Law (Expert Draft)", China Civil and Commercial Law Network: http://www.civillaw.com.cn/lw/l/?id=36127, accessed on November 5, 2019.
- Fan Wei, “Reconstructing the Path of Personal Information Protection in the Big Data Era”, Global Legal Review, No. 5, 2016, pp. 92-115.
- https://www.legislation.gov.au/Details/C2014C00076, accessed on November 5, 2019.
- http://law.npc.gov.cn:8081/FLFG/flfgByID.action