CADERNOS DE DEREITO ACTUAL
www.cadernosdedereitoactual.es

© ***Cadernos de Dereito Actual*** Nº 28. Núm. Ordinario (2025), pp. 44-62

·ISSN 2340-860X - ·ISSNe 2386-5229

Quantitative jurisprudence: dynamic balancing framework of personal information protection via information entropy and Alexy's formula

Qizhen Yang[1]
Law School, Shanxi University

Abstract: China's personal information protection system mainly unfolds around the protection of personal information rights and the realization of data interests. However, this system faces two major predicaments in practice: the definition of the protected objects and the balance between rights and interests. Whether information belongs to personal information needs to be judged specifically in specific usage scenarios. Personal information simultaneously carries the dual demands of data flow and rights protection, and a balance needs to be achieved. The entropy weight model based on information entropy theory can calculate and describe the identification ability of personal information, providing objective parameters for judgment. By substituting the calculation results of the entropy weight model into the Alexy weight formula, the balance between personal information rights and data flow interests in

[1] Master of Law from Shanxi University, with main research interests in digital law, artificial intelligence governance, intellectual property rights, and machine ethics. Orcid: https://orcid.org/0009-0002-4705-2839. E-mail: m19935366936@163.com

dynamic scenarios can be analyzed. This article proposes a method to assist in determining the legal definition of the object and the dynamic balance of rights and interests through calculation conclusions by adopting an interdisciplinary research approach, and presents an effective research paradigm for personal protection.

Keywords: Personal Information; Information Entropy; Weighing Rule; Rights and Interests Balance.

1. Introduction

The protection of personal information is an important issue in today's world. Its importance is not only reflected in the protection of personality rights, but also in the efficiency of the entire society. The Civil Code of the People's Republic of China (hereinafter referred to as the "Civil Code") includes personal information in the "Book Four: "Personality Rights" are separately listed in Chapter VI Right of Privacy and Protection of Personal Information in terms of the system structure, which means that the legislation clearly defines personal information as carrying fundamental personality rights, and is distinguished from other Personality Rights such as Right of Reputation and Right of Honor as well as Right of Likeness and placed at the same level.[2] The enactment of the Personal Information Protection Law of the People's Republic of China (hereinafter referred to as the "PIPL")further clarifies the principles of personal information protection and the rules for processing personal information, clarifies the scope of rights and obligations in the process of personal information processing, and improves the personal information protection mechanism.[3]

It should be noted that the concept of "personal information rights" is relatively narrow, referring to the rights that individuals have over their personal data as stipulated in the Personal Information Protection Law. However, the subject matter discussed in this article, namely the concept of "personal information protection", not only encompasses the rights that individuals have over their personal information, but also includes the obligations of data processors and the legitimate interests they obtain from data flows. It further encompasses the regulatory requirements, compliance mechanisms, and enforcement procedures, among other systematic frameworks, stipulated in the PIPL.

However, in the personal information protection system established by the Personal Information Protection Law, there are still two problems to be solved in order to protect personal information rights and the interests of all parties involved in data flow. The first is the issue of defining the object. Article 4 of the Personal Information Protection Law defines personal information, but the scope, applicability and interpretation boundaries of terms such as "identifiable", "identified" and "related to" are still not clear enough in terms of legal clarity and conceptual precision.[4] The

---

[2] Article 1,034 of the Civil Code: The personal information of natural persons is protected by law.
Personal information is various information recorded electronically or in other forms that can identify a specific natural person separately or in combination with other information, including a natural person's name, date of birth, identity card number, biological recognition information, address, telephone number, e-mail address, health information, and whereabouts information, among others. Private information in personal information shall be governed by the provisions on privacy right; where there are no provisions, the provisions on the protection of personal information shall apply.

[3] LI, Q., JIANG, T., & FAN, X. "Examining Sensitive Personal Information Protection in China: Framework, Obstacles, and Solutions." Information & Culture, v. 58, n. 3, 2023, p. 247-273.

[4] Personal Information Protection Law Article 4：“Personal information” means all kinds of information related to identified or identifiable natural persons that are electronically or otherwise recorded, excluding information that has been anonymized.
Personal information processing includes, but is not limited to, the collection, storage, use, processing, transmission, provision, disclosure, and deletion of personal information.

second is the conflict between the interests of all parties involved in data flow and the protection of personal information rights, which further increases the difficulty of personal information protection. To effectively solve these problems, this article will discuss in the order of "defining the object of rights" and "achieving rights balance". It examines personal information rights from three dimensions: ontology, epistemology and methodology. From the ontological dimension, it explains the mathematical logic of personal information; from the epistemological dimension, it combines the computational logic of personal information with legal theory; and based on the conclusions of the first two parts, it constructs a model from the methodological perspective to balance personal information rights and the interests of data flow.

2. The definitional dilemma of personal information and attempts at judgment-support parameter models

When discussing the issue of personal information protection, the first problem to be addressed is the definition of the object. The definition of the object is not only the logical starting point of personal information protection research but also the foundation for ensuring the effectiveness of subsequent rights balance analysis.

2.1. Methods of defining the subject matter of personal information

This article first reviews the evolution of the definition of personal information in Chinese legal documents. From the perspective of the chronological order of the release of legislative documents, the scope of the definition of personal information shows a gradually expanding trend. From the perspective of the definition method, the definition of personal information in legislation has been constantly evolving, mainly divided into two mainstream definition methods: "identification definition method" and "relation definition method".[5]

Firstly, according to the evolution process of the definitions in Table 1, it can be seen that the scope of personal information has been continuously expanding. It has developed from limited information directly identifying a citizen's identity to a broader range of information that can identify an individual when combined with other information. Subsequently, its scope has further expanded to cover various types of information reflecting the activities of specific natural persons. In the subsequent Civil Code, the enumeration method was added, and the latest Personal Information Protection Law defines it as information related to identified or identifiable natural persons. This definition adopts the "related to", "identified" and "identifiable" definition model, further expanding the scope of personal information. Nowadays, the latest definition of personal information can cover a very wide range of information, which is conducive to the protection of personal information rights, but its definition method also brings greater complexity to the application and interpretation in judicial practice.

Secondly, in terms of the definition methods of personal information, following the chronological order, legislative documents have undergone a transformation from mainly adopting the "identification definition method" to the concurrent use of the "identification definition method" and the "relation definition method". In the application of the "identification definition method", it has gone through a process from mainly using direct identification to the concurrent use of direct and indirect identification. The latest legislation adopts a definition model that combines the concepts of already identified and identifiable, and simultaneously uses the "relation definition method". The "Decision on Strengthening the Protection of Network Information" of the Standing Committee of the National People's Congress adopts the direct definition method, only considering information that can directly identify a

[5] HE, B. "On the Definition of Personal Information Concept." Information Communication Technology and Policy, 2018, n. 6, p. 38-42.

citizen's personal identity as personal information. Direct identification focuses more on the one-to-one correspondence between information and a specific individual, and the scope of personal information defined in this way is relatively limited, such as names and ID numbers. The "Cybersecurity Law of the People's Republic of China", the "Interpretation on Several Issues Concerning the Application of Law in Handling Criminal Cases of Infringing upon Citizens' Personal Information" issued by the Supreme People's Court and the Supreme People's Procuratorate, and the "Civil Code of the People's Republic of China" all adopt a definition model that combines direct and indirect identification. Indirect identification is defined as "information that can identify a specific natural person when used alone or in combination with other information", where "other information" is a prerequisite for correctly understanding indirect identification. However, Chinese legal documents have not provided a definition or scope for "other information". This definition method expands the scope of personal information but also brings a certain degree of ambiguity. Within an extremely wide range of information, there exist various combinations that can be associated with individuals. Broadly speaking, any information may be combined with other information to identify a specific social individual.[6] Moreover, the "other information" that can be combined with the judged information itself must have a certain identification function. During the identification process, the roles played by various types of information are difficult to distinguish, and their contributions cannot be quantified.[7] If other information inherently possesses high or complete identifying capabilities, the definition of indirect identification could lead to confusion in practice and potentially unreasonably expand the scope of personal information.

As the latest personal information protection law, PIPL simultaneously adopts the "identification definition method" and the "relation definition method", using the three terms "related to", "identified", and "identifiable" to describe personal information. These terms define personal information based on the two core concepts of identification and relation.[8] However, legal documents and relevant judicial interpretations have yet to provide effective interpretations of these two concepts and three terms, and there are still difficulties in their interpretation and application in practice.

As China has extensively drawn on the legislative content of the European Union at each stage of its personal information legislation, especially in the PIPL, the definition of personal information has borrowed from the content of Article 4 of the EU's General Data Protection Regulation (GDPR): (1) 'personal data' means any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person[9,10]. Therefore, this paper extends the discussion on this definition in the GDPR

---

[6] Ding, X. "On the Uncertainty of the Concept of Personal Information and Its Legal Responses." *Journal of Comparative Legal Studies*, v. 183, n. 5, p. 46-60.

[7] LAH, F. "Are IP addresses personally identifiable information?" *ISJLP*, v. 4, n. 3, 2008, p. 681.

[8] CHENG, X. "Understanding and Application of Personal Information Protection Law." China Legal Publishing House, Beijing, China,2021.

[9] EUROPEAN PARLIAMENT & COUNCIL OF THE EUROPEAN UNION. "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)." Official Journal of the European Union, v. L119, n. 1, 2016, p. 1–88.

[10] Article 4 of the Personal Information Protection Act: Personal information refers to any information recorded in electronic or other forms that is related to identified or identifiable natural persons, excluding information that has been anonymized. The processing of personal information includes the collection, storage, use, processing, transmission, provision,

and the corresponding academic research to deepen the analysis of the model of personal information definition.

Table 1. The definitions of personal information in different legislative documents in China.

Document name and effective time	**Number**	**Content**
Decision of the Standing Committee of the National People's Congress on Strengthening the Protection of Network Information, December 28, 2012	Article 1 Paragraph 1	The state protects electronic information that can identify the personal identity of citizens and that involves their personal privacy.
Cybersecurity Law of the People's Republic of China, June 1, 2017	Article 76 Item 5	Personal information refers to all kinds of information that can identify the personal identity of a natural person either alone or in combination with other information, recorded in electronic or other forms. This includes but is not limited to a natural person's name, date of birth, ID number, personal biometric information, address, and phone number.
Interpretation of Several Issues Concerning the Application of Law in Handling Criminal Cases of Infringing upon Citizens' Personal Information by the Supreme People's Court and the Supreme People's Procuratorate, June 1, 2017	Article 1	All kinds of information recorded in electronic or other forms that can identify the identity of a specific natural person alone or in combination with other information, or reflect the activities of a specific natural person, including name, ID number, communication contact information, address, account password, property status, travel trajectory, etc.
Civil Code of the People's Republic of China, January 1, 2021	Article 1034 Paragraph 2	Personal information is various information recorded electronically or in other forms that can identify a specific natural person separately or in combination with other information, including a natural person's name, date of birth, identity card number, biological recognition information, address, telephone number, e-mail address, health information, and whereabouts information, among others.
Personal Information Protection Law of the People's Republic of China, November 1, 2021	Article 4 Paragraph 1	"Personal information" means all kinds of information related to identified or identifiable natural persons that are electronically or otherwise recorded, excluding information that has been anonymized.

The definition of personal information in the GDPR largely follows that of 'personal data' in Directive 95/46/EC, which states: 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity; Therefore, documents that interpret Directive 95/46/EC are helpful for understanding the various elements in the definitions. Article 29 Data Protection Working Party (2007) pointed out that for the "RELATING TO" element, apart from data that can obviously be regarded as related to

disclosure, and deletion of personal information.

an individual, for data to be considered as "relating" to an individual, either a "content" element or a "purpose" element or a "result" element should be present. It emphasized that these three elements (content, purpose, result) must be regarded as alternative conditions, not cumulative ones. The document also provided relevant examples.[11] Generally, a natural person can be regarded as 'identified' when, within a group of individuals, he or she can be distinguished from all other members of the group. Accordingly, the natural person is 'identifiable' when, although the person has not yet been identified, it is possible to do so (that is the meaning of the suffix "-able"). The above explanation provides more detailed definitions of the relation and identification elements, offering clearer guidance for the judicial practice process.

The adoption of the "relation definition method" has expanded the scope of personal information. This is because in the era of the Internet and big data, many pieces of information cannot be directly or indirectly associated with an individual's name. However, as long as the relevant information is associated with a specific individual, it may have a significant impact on that person.[12] However, this expansion will further complicate the application of the definition of personal information and may lead to controversial results. Firstly, the judgment mode of the "relation definition method" is dependent on the "identification definition method", that is, the identified or identifiable natural person is the object of "relating to", and the identifiable natural person includes the process of being directly or indirectly identified. In practice, personal information exists in various forms and may be combined in various ways. Indirect identification itself is a dynamic and complex process, and the analysis and interpretation process of the content, purpose, and result elements further expand this complexity and may lead to controversial results. Judgments made through the above elements may also be influenced by subjective tendencies.

In academic discussions in China, apart from the "identification definition method" and the "relation definition method", scholars are actively exploring the Scenario-based definition method.[13] Purtova also points out that the core of identity recognition is regarded as the process or result of distinguishing individuals within a group.[14] In the emerging Scenario-based definition method, personal information is not a static concept that can be predefined, but rather a process of dynamic judgment during usage.[15] Therefore, personal information should be defined within the context of specific dynamic scenarios. The "scenario-based definition method" is essentially a framework composed of "information content, information usage scenarios, information usage purposes, information security status, and information rights balance". The fundamental logic of the scenario-based definition method lies in defining personal information within a unified system constituted by natural persons, information processors, information content, and usage scenarios, and analyzing the balance of rights and interests. The scenario-based definition method does not deny the "identification definition method" and the "relation definition method", but rather unifies them.[16] It determines whether information belongs to personal information by evaluating the dynamic process of identifying and relating individuals in specific

---

[11] Article 29 Data Protection Working Party. (2007, June 20). Opinion 4/2007 on the concept of personal data (WP136). European Commission.

[12] Borgesius, F. J. Z. (2016). Singling out people without knowing their names—Behavioural targeting, pseudonymous data, and the new Data Protection Regulation. *Computer Law & Security Review*, v. 32, n, 2, 2016, pp. 256-271.

[13] XIAO, X. "An analysis and construction of personal information rights." *Chinese Journal of Law*, v.45, n. 6, 2023, p. 73.

[14] PURTOVA, N. "From Knowing by Name to Targeting: The Meaning of Identification under the GDPR." *International Data Privacy Law,* v. 12, n. 3, 2022, p. 163-183.

[15] NISSENBAUM, H. "Privacy as contextual integrity." *Washington Law Review*, v. 79, n. 119, 2004, p. 119-157.

[16] SMITH, H.J., Dinev, T., Xu, H. "Information privacy research: An interdisciplinary review." *MIS Quarterly*, v. 35, n. 4, 2011, 989-1015.

scenarios through the use of specific information, and on this basis, adopts the sequence of "scenario analysis - risk assessment - interest balance" to analyze the balance between data flow and personal information rights.

2.2. An attempt at entropy weight parameters in the scenario-based definition method

To define personal information through the Scenario-based definition method, it is necessary to analyze all elements in dynamic scenarios, including information content, information combination, and the context in which an individual is identified, while minimizing the interference of subjective judgment. By drawing on the mathematical definition of information, it can be found that information is measured based on the uncertainty of the system it is in, which is consistent with the logic of the Scenario-based definition method. To precisely define personal information in dynamic scenarios, an interdisciplinary approach should be adopted, closely integrating mathematical logic with legal theory, and attempting to find objective parameters that are not influenced by preconceived value judgments, and then draw legally significant conclusions from them.

The essence of personal information is information, and information can be quantitatively expressed through mathematical formulas. By using this parameter, the ability of information to identify and relate individuals in specific scenarios can be precisely described, providing a basis for determining whether it constitutes personal information. Claude Shannon, the "father of information theory," believed that "information is that which eliminates uncertainty."[17] If uncertainty is eliminated, information is obtained. If all uncertainty in the original system is eliminated, all information is obtained; if only part of the uncertainty is eliminated, partial information is obtained. If none of the original uncertainty is eliminated, no information is obtained. Shannon proposed the "information entropy" theory to describe the various uncertain states that information sources may be in. "Entropy" was originally a concept in thermodynamics used to describe the degree of disorder in a system.[18] Later, Boltzmann applied statistical principles to study the probability of molecular motion and the arrangement of physical quantities. Shannon borrowed this theory and defined the average amount of information remaining after removing redundant content as information entropy. Based on this theory, humanity invented ways to express information digitally, developed digital communication technologies, and ushered in the digital age.

The theory of "information entropy" proposed and solved the problem of quantifying information, and also provided a formula for calculating information entropy. A signal source has n possible values: $U_1 \ldots U_i \ldots U_n$, each corresponding to a probability $P_1 \ldots P_i \ldots P_n$, and the occurrence of various symbols is independent of each other. In this case, the average uncertainty of the signal source is the statistical average of the uncertainty of a single symbol, which is called information entropy.

$$H\ （U）= E\left[-\log \mathrm{p}_{\mathrm{i}}\right]=-\sum_{\mathrm{i}=1}^{\mathrm{n}} \mathrm{p}_{\mathrm{i}} \log \mathrm{p}_{\mathrm{i}}$$

---

[17] SHANNON, C.E. "The mathematical theory of communication." *The Bell System Technical Journal*, v. 27, n. 3, 1948, p. 379-423.

[18] Entropy (originally a thermodynamic function, later developed into a measure of the disorder of a system, is a function describing the thermodynamic state of a system. The term "entropie" was coined by German scientist Rudolf Julius Emanuel Clausius (1822–1888) in his 1865 paper "On Several Forms of the Principal Equations of the Mechanics of Heat Suitable for Application" (Über verschiedene für die Anwendung bequeme Formen der Hauptgleichungen der mechanischen Wärmetheorie). In 1877, Boltzmann expressed the magnitude of a system's disorder using the following relationship: $S \propto \ln\Omega$, known as the Boltzmann entropy formula.

The unit of information quantification is the bit (bit), where 1 bit = 2^2. It describes the choice made between two possible states, meaning that 1 bit of information describes a system with two equally probable states. This formula mathematically describes the relationship between information and the system it is in. In an information system, the amount of information contained in a certain state is consistent with its probability of occurrence. In a communication scenario, the specific signal emitted by the signal source is uncertain, and information entropy measures them based on their probability of occurrence. If the probability of occurrence is high, the possibility of occurrence is large, the uncertainty is low, and the amount of information contained is small. Conversely, if the probability of occurrence is low, the possibility of occurrence is small, the uncertainty is high, and the amount of information contained is large. If the information is completely certain, its information quantity is 0. Shannon's information entropy formula quantifies information and expresses it in digital form, thus enabling calculation. The calculation logic is the foundation of digital rationality, and its orderly presentation can also lay the foundation for social legitimacy and ethical rules. By comparing Shannon's definition of information with the legal definition of personal information, it can be found that the logical connotations of the two are consistent. In the Scenario-based definition method, the "usage scenario", "information content", and the ability of information to identify and relate individuals are the core elements for determining whether information is personal information. Expressed in mathematical language, the "usage scenario" of information existence is an information system with probability, and the information content is information with a specific occurrence probability. The ability of information to identify and relate individuals is determined by the information content to determine the specific state of the system.

In the Scenario-based definition method, "usage scenarios" refer to the groups in which individuals are to be identified, and the "information content" and the ability to identify and relate individuals can be precisely calculated within the group information set. Due to the possible combination of various information in specific scenarios, the entropy weight model should be adopted to complete this process and describe the identifying and relating individuals of different content information.

2.3. Defining personal information parameters in the construction of the "entropy weight model"

Based on the above requirements, this paper adopts entropy weight as an objective parameter to judge the individual identification ability of information. This choice is based on the following assumptions. First, identification is a dynamic process, whose essence is to distinguish a specific individual within a group. Therefore, the number of individuals in the group and their respective information composition are definite, which simulates the situation where information processors have a certain amount of personal information and use it. Secondly, the identification ability of information to an individual is related to its content, that is, to objectively describe through data to what extent a specific piece of information in a specific group data set can identify a specific individual.

Model construction:

In order to comply with the personal information protection requirements, this paper utilizes a random data generation platform. Given that the principal objective of the model study is to analyze the value patterns of personal information in a particular scenario and to explore protection methods, the random generation of the model will not affect the conclusions of the research results due to the use of non-actual data.

The following table presents a variable design.

As shown in Table 2, the utilization of the Mockaroo random data generation platform facilitates the simulation of a personal information database, in which four parameters are randomly assigned to 1,000 individuals. These parameters include

gender (male or female), age (range 20—30), month of birth (1—12), and education level (high school, college, master's degree or above). The construction of an entropy-weighted model is predicated on the database. The analysis examines the ability of different types of personal information to identify and associate individuals in this particular scenario. Furthermore, it explores the value of personal information and the methods employed for its protection.

Table 2. Variable design.

Variable	Value range/Levels	Distribution logic
Gender	Female, Male Male	Random
Age	20–30 years	Uniform distribution
Birth Month	1 (Jan)–12 (Dec)	Uniform across calendar months
Education	High School, Bachelor, Master+	Random

The entropy weight method was employed to objectively determine the weights of four indicators: gender, birth month, age, and education level. The implementation process consisted of six key steps, executed in Stata 17.0 (code available upon request).

Categorical variables were converted to numerical representations to facilitate quantitative analysis:

Gender: Binary encoded as 0 = female, 1 = male using recode with explicit label definitions.

Education Level: Ordinal encoding 1 = High school, 2 = Bachelor, 3 = Master or above to preserve hierarchy.

The above-mentioned variables are presented in Table 3:

Table 3. Variable definitions.

Variable	Type	Description/Encoding	Example
Gender	Binary	0 = Female, 1 = Male	1 (Male)
Educational Level	Categorical	1 = High school, 2 = Bachelor, 3 = Master+	2 (Bachelor)
Age	Numerical	20-30 years	25

Data Standardization:

All indicators were treated as positive-directional variables (higher values indicate better outcomes). A min-max normalization was applied to eliminate scale differences:

$$x_{norm} = \frac{x - \min(x)}{\max(x) - \min(x)}$$

Descriptive statistics of raw variables (Table 4) confirmed the necessity of normalization, with scales ranging from 0,1 (gender) to 1,12 (birth month).

Table 4. Descriptive Statistics of Raw Variables (N=1,000).

Variable	Mean	Std. Dev.	Min	Max
Gender (0/1)	0.502	0.500	0	1
Birth Month	6.542	3.531	1	12
Age	24.97	3.142	20	30
Education Level	1.959	0.817	1	3

Entropy Calculation:

For each standardized variable x_{norm} ,the information entropy E_j was computed as:

$E_j = -\frac{1}{\ln N}\sum_{i=1}^{N} p_{ij} \ln p_{ij}$, where $p_{ij} = \frac{x_{ij}}{\sum_{i=1}^{N} x_{ij}}$

Zero-value handling: Instances with $p_{ij} = 0$ were replaced with $\epsilon = 10^{-6}$ to avoid undefined logarithmic operations.

Effective sample size: $N = 1{,}000$ observations ensured stable entropy estimates.

Weight Determination:

The divergence coefficient D_j and final entropy weight w_j were derived as:

$$D_j = 1 - E_j,\ w_j = \frac{D_j}{\sum_{j=1}^{4} D_j}$$

Validation confirmed the weights summed to unity $(\sum w_j = 1)$,ensuring methodological consistency.

Table 5 presents the calculation results of the variables. In this model, the entropy value reflects the degree of dispersion of different sample data under the same indicator. The larger the entropy value (closer to 1), the more the data of all samples under this indicator are highly consistent (with a smaller degree of dispersion), and the less information it provides. Divergence is the complement of entropy and is used to quantify the degree of variation or information utility of an indicator. The larger the Divergence (closer to 1), the smaller the entropy value, indicating significant differences in the data of this indicator and a strong ability to distinguish samples. The smaller the Divergence (closer to 0), the larger the entropy value, indicating high consistency in the data and a weak ability to distinguish. The entropy weight is the normalized result of the coefficient of variation. The entropy weight is the result of objective weighting, reflecting the relative distinguishing ability of the indicator under data-driven conditions. The larger the entropy weight, the higher the distinguishing degree of this indicator, and the greater the weight it is assigned in the evaluation. That is, data with a higher entropy weight have a stronger ability to distinguish specific individuals.

Table 5. Calculation result.

Variable	Description	Entropy (ej)	Divergence (dj)	Weight (wj)
Gender	0 = Female, 1 = Male	0.589	0.411	0.4106
Education Level	1 = High school, 2 = Bachelor, 3 = Master+	0.705	0.295	0.2954
Birth Month	1-12(Calendar month)	0.853	0.147	0.1474
Age	20-30 years	0.853	0.147	0.1467

3. The balance between personal information rights and data flow rights in personal information protection

The primary issue in personal information protection is to solve the problem of defining personal information. In this part, we will draw legally significant conclusions based on the objective parameters obtained from the aforementioned entropy weight model. The second important issue is that the personal information protection system needs to balance the contradiction between personal information rights and the rights of data flow circulation. To achieve the above two purposes, the author will attempt to use Alexy's balance formula to draw legally significant value judgment conclusions.

3.1. The conflict between personal information rights and data flow rights

There are mainly two theoretical tendencies regarding the essence of personal information. The first one regards personal information as property, considering it a special form of property owned by users, who control their personal information based on the rights they have over this special property. The theoretical basis for this view comes from economics. Scholars holding this view believe that the market is the most effective regulatory mechanism, with better regulatory capabilities and operational efficiency than the government. The value of property reflects the value of personal information and can be adjusted through the market.

Prominent supporters of this view include Professor Jerry Kang and the renowned American judge Richard Posner.[19] Posner, one of the founders of law and economics, believes that legal protection of personal information is inefficient and that special protection for it in the information age is "completely unnecessary".[20] Legal

[19] KANG, J. "Information privacy in cyberspace transactions." *Stanford Law Review,* v. 50, n. 1, 1997, p. 1193-1254.

[20] POSNER, R.A. "The economics of privacy." *The American Economic Review,* v. 71, n. 2, 1981,

protection of information hinders its circulation, and obstructed information flow not only increases the cost of information transmission but also fosters more fraudulent behavior. From a market economy perspective, the choice between protecting the rights of businesses over information and the interests of users over information should be left to the market. This view does not distinguish between the content of information and the purpose for which it is obtained. Instead, it measures the value of information based on the price people are willing to pay to achieve their goals. If someone needs personal information, they must purchase it. The balance between the price of information and the benefits that can be obtained after acquiring it will determine whether to purchase it. As long as a third party offers a higher price, it can become the new owner of the information. Harper holds that treating information as property has raised some concerns and challenges, but the common handling of personal information aligns with multiple property theories, and information has already acquired the characteristics of property in the common law sense.[21]

However, there are still some predicaments in the institutional design of personal information from an economic perspective, including the distinction in nature between information and property, as well as the inability to unify the framework and conclusions of economic analysis methods and results. From a technical perspective, Nekit pointed out that the characteristics of data, such as non-exclusivity and infinite replicability, conflict with traditional property rights and are incompatible with them.[22] The core of the economic analysis lies in assessing the economic value and consequences of protecting and disclosing personal information. However, no consensus has been reached on this issue. Firstly, the problem of personal information with economic significance emerges in an extremely broad and complex context, making it difficult to describe it with a single unified economic theory. Secondly, both in theory and in empirical situations, the protection of personal information may either enhance or undermine the welfare of individuals and society. Thirdly, in the digital economy, consumers are often in a situation of incomplete or asymmetric information, being unaware of when their data is collected, the purpose of collection, and the possible consequences, which severely hinders their ability to make informed decisions.[23] Furthermore, economic theory suggests that the protection of individual privacy can have varying impacts on overall welfare, depending on specific conditions and assumptions. Thus, addressing privacy concerns necessitates finding a balance between information sharing and concealment, one that aligns with the interests of data subjects as well as the broader society, including other data subjects and potential data holders.[24]

This view has another obvious problem. The rights that individuals enjoy over information should not be entirely described by market bidding mechanisms driven by the interests of other entities. Chesnokova emphasizes that personal information is inseparable from human dignity and autonomy, being an extension of one's personality rather than a common commodity. The property framework fails to encompass individuals' psychological needs for privacy.[25] Moral and ethical bottom lines cannot be measured by money. The freedom and dignity embodied in personal information are important components of human rights, and human rights are the

---

p. 405-409.

[21] HARPER, J. "Personal Information is Property." *SSRN Electronic Journal*, 2024.

[22] NEKIT, K. "The (im)possibility of personal and industrial (machine-generated) data to be subject to property rights." *International Journal of Law and Information Technology*, v. 32, 2024.

[23] ACQUISTI, A.; TAYLOR, C.; WAGMAN, L. "The economics of privacy." *Journal of Economic Literature*, v. 54, n. 2, 2016, p. 442-492.

[24] ACQUISTI, A. "The economics of personal data and the economics of privacy." *Economics*, v. 11, 2010, p. 24.

[25] CHESNOKOVA, L. V. "Information privacy: protecting freedom and individual autonomy." *The Digital Scholar Philosopher s Lab*, v. 4, n. 2, 2021, p. 145-157.

most basic rights that every person should enjoy and cannot be subject to market adjustments. Just as the law prohibits the deprivation of another person's life and freedom, it is necessary to prohibit the buying and selling of life and freedom. This utilitarian perspective fails to distinguish between the value hierarchy of basic human rights and commercial interests, posing significant ethical and moral risks.

The second perspective holds that personal information embodies the right to autonomy, meaning that individuals should have control over their information. Alan Westin argues that individuals should have absolute control over all aspects of information dissemination, including its scope, timing, location, context, and purpose. The theory of personal information as an autonomous right originates from Locke's liberalism, which asserts that the law should guarantee the basic dignity and equality of all individuals.[26] The means to achieve equality and dignity is for individuals to exercise control over their information, thereby realizing basic human dignity and safeguarding human freedom. Elvira systematically expounds the legal theory of the "right to information self-determination" in the European Union, emphasizing that it is a necessary tool for maintaining a vibrant democracy.[27] The protection of personal information can shield individuals from the threat of "personality transparency", and prevent the "covert manipulation" caused by the weakening of autonomous decision-making ability when technology generates personal profiles through inferring behavioral data (such as personalized targeted push).[28]

Personal information embodies the dignity and freedom inherent in human rights, but the efficient flow of information is equally necessary for social operations and economic development. The contradiction between individuals' control over information and the demand for data circulation and use is reflected in the opposition between these two schools of thought.[29] Chinese scholar Xu Ming argues that personal information in the digital age cannot exist as an absolute secret but should be in an intermediate state between secrecy and public disclosure.[30] Personal information is not an absolute right but should be recognized as a relative right, a rule governing the management of information order. The dimension of personality protection provides individuals with a "non-public area of life" through personal information protection, meeting the deep-seated human needs for secrecy and opacity of personality. It does not mean completely hiding one's life but rather selectively disclosing it through access control[31].

Under the two mainstream viewpoints mentioned above, neither can perfectly solve the interpretation of the nature of personal information nor the construction of protection methods. However, it can be found that the focus of the problems in both theories lies in the balance construction between the circulation interests of personal information and the direct protection of personal information rights.

In specific usage scenarios, there is a fundamental conflict between the two major forces in information systems. On the one hand, there is the protection of users' personal information; on the other hand, there is the identity recognition technology based on data flow for association and personalized services.[32] Due to the diverse and

---

[26] AUSTIN, L. M. "Re-reading Westin." *Theoretical Inquiries in Law*, v. 20, n. 1, 2019, p. 53-81.
[27] TALAPINA, E. "The Right to Informational Self-Determination: On the Edge of Public and Private." *Legal Issues in the Digital Age*, v. 3, n. 4, 2022, p. 34-51.
[28] VOLD, K., & WHITTLESTONE, J. "Privacy, Autonomy, and Personalised Targeting: Rethinking How Personal Data Is Used." In Data, Privacy, and the Individual in the Digital Age, 2019.
[29] FAINMESSER, I.P., GALEOTTI, A., MOMOT, R. "Digital privacy." *Management Science,* v. 69, n. 6, 2023, p. 3157-3173.
[30] XU, M. "Privacy Crisis and Tort Law Response in the Era of Big Data." *China Legal Science*, v. 2017, n. 1,p.130-149.
[31] CHESNOKOVA, L. V. "Information privacy: protecting freedom and individual autonomy." *The Digital Scholar Philosopher s Lab*, v. 4, n. 2, 2021, p. 145-157.
[32] WACHTER, S. "Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR." *Computer Law & Security Review*, v. 34, n. 3, 2018, p.

complex usage scenarios, people always handle personal information from their own perspectives and in their own ways. They often do not know what information they are sharing or how it will be used. Even in the rare cases where they fully understand the consequences of sharing, it is still difficult for them to determine their preferences. The asymmetry between information providers and processors directly leads to information security risks and distrust (Acquisti, Brandimarte, and Loewenstein, 2015).[33]

3.2. Definition of personal information and balancing of rights in specific use cases

In specific use cases involving personal information, the first issue to address is the definition of personal information, i.e., how to determine whether information constitutes personal information. The second issue is the balancing of rights related to personal information, i.e., analyzing and achieving a balance between information protection and data flow.[34] The definition of personal information should be determined on a case-by-case basis using information entropy parameters, and the balancing of rights must also be achieved in specific use cases.[35]

The need for rights balance is the manifestation of the principle of proportionality in rights conflicts. In specific usage scenarios, based on information content and system uncertainty, "information entropy" can calculate whether information possesses and to what extent it possesses "identification" and "association" capabilities, thereby objectively determining whether it constitutes personal information. The purpose of information use can also be calculated as specific 'identification' and "association" metrics. "Information entropy" can objectively measure the demand for information use, determine the minimum information standard required to achieve the purpose of information use, and serve as a reference for balancing rights and interests. The method for balancing rights and interests should adopt the "balancing rule" proposed by German jurist Alexy[36]. A weighting formula designed based on "principal conflicts" should be used as the judgment method.[37] In specific usage scenarios, the greater the need to infringe upon or destroy one right, the higher the importance of protecting the other conflicting right, thereby achieving a stable balance between them.[38] Similarly, in an already balanced state, if the necessity of achieving a right increases, the importance of the corresponding right must be proportionally amplified to counteract the infringement[39]. Through the balance rule conceived by Alexy, the principle of proportionality can be better realized.[40] The formula proposed by Alexy can be used to judge the excessive

436-449.

[33] ACQUISTI, A.; BRANDIMARTE, L.; LOEWENSTEIN, G. "Privacy and human behavior in the age of information." *Science*, v. 347, n. 6221, 2015, p. 509-514.

[34] CHEN, L., HUANG, Y., OUYANG, S., XIONG, W. *The Data Privacy Paradox and Digital Demand (No. w28854);* National Bureau of Economic Research, Cambridge, MA, USA, 2021.

[35] BEESLEY, S.J., POWELL, A., GROAT, D., BUTLER, J., HOPKINS, R.O., ROZENBLUM, R., BROWN, S.M. "Evaluating the balance between privacy and access in digital information sharing." *Critical Care Medicine,* v. 50, n. 2, 2022, p. e109-e116.

[36] ALEXY, R. "The weight formula." *In Rights: Concepts and Contexts;* Routledge, 2017. pp. 539–558.

[37] KORGANBEKOVA, M., ZUBER, C. "Balancing user privacy and personalization." *Work in Progress*, 2023, 6.

[38] ALEXY, R. "The weight formula." *In Rights: Concepts and Contexts;* Routledge, 2017. pp. 539–558.

[39] BERRESHEIM, L.H.M. Balancing Privacy and Other Rights. Doctoral dissertation, University of Amsterdam, Amsterdam, 2024.

[40] JANEBOVÁ, R.; RIGEL, F. "Using Robert Alexy's law of balancing in social work decision-making." *European Journal of Social Work*, v. 5, 2025, p. 1-11.

disproportion and trade-offs among different rights in specific risk scenarios.[41] In the continuous exploration, the Alexy formula has also demonstrated its advantages, especially the compatibility of the value judgment process and the technical path. Therefore, it has been widely applied in the decision-making process of various design algorithms, including ethical dilemmas in autonomous driving.[42] The specific weighting formula is:

$$W_{ij} = \frac{P_i}{P_j} = \frac{I_i \cdot W_i \cdot R_i}{I_j \cdot W_j \cdot R_j}$$

W_{ij} represents the weighting ratio of right P_i relative to right P_j. In a specific context, when W_{ij} is greater than 1, it indicates that P_i is more important and should be prioritized over P_j. If W_{ij} is less than 1, it indicates that P_j is more important and should be prioritized over P_i. When W_{ij} is equal to 1, there is no priority between them, meaning that the two rights are in a state of equilibrium. The weighting formula has broad application prospects in the calculation of personal information rights balancing [43].

The parameter I_i represents the extent of harm to P_i, which is the reduction in uncertainty within the information system, i.e., the system's ability to identify and associate information with specific individuals. The formula has three parameters to characterize the degree of damage: severe (S), moderate (M), and mild (L). S represents severe damage, meaning that the information content can almost eliminate the uncertainty in the system and accurately identify individuals. For instance, the ID numbers that citizens possess, these data codes form a one-to-one correspondence with individual citizens. In other words, once the collector knows a citizen's ID number, the citizen's identity is no longer uncertain and is completely determined. M represents moderate damage, meaning that the uncertainty in the information system has been reduced but not eliminated. The information still has some ability to identify individuals within the system, but cannot accurately identify specific individuals. For instance, in a class composed of multiple people with an equal gender ratio, an individual's gender information can eliminate half of the individuals, but it cannot completely eliminate uncertainty and cannot identify a specific individual in the class. L represents minor damage, indicating that a small amount of uncertainty has been eliminated within the system, but the system cannot identify individuals. For instance, in a class of the same grade, 98% of the students are 14 years old. This piece of personal information, "14 years old", can only eliminate 2% of the subjects, reducing a very small amount of system uncertainty and having a very weak connection with a specific individual. Such information, due to its extremely limited content, cannot perform the functions of "identification" and "association" and can be considered non-personal information. Therefore, minor damage (L) is not included in the calculation. M and S correspond to the values 2^0 and 2^1, respectively.

I_j indicates the importance of P_j, i.e., the importance of obtaining personal information for the counterpart, expressing the necessity of identifying individuals. The specific measurements remain severe (S), moderate (M), and mild (L). L indicates unimportant, meaning there is no urgent need to obtain personal information, and not collecting personal information does not affect contract

---

[41] NOVELLI, C.; CASOLARI, F.; ROTOLO, A.; TADDEO, M.; FLORIDI, L. "AI risk assessment: a scenario-based, proportional methodology for the AI act." *Digital Society,* v. 3, n. 1, 2024, p. 13.

[42] TANG, J.; LUO, X.; CHEN, J.; YUAN, Y.; LOO, J. "An ethical decision making algorithm for autonomous vehicles during an inevitable collision." *In Proceedings of the 2024 4th International Conference on Big Data, Artificial Intelligence and Risk Management*, 2024, p. 1077-1081.

[43] POPOWICZ–PAZDEJ, A. "The proportionality principle in privacy and data protection law." *Journal of Data Protection & Privacy,* v. 4, n. 3, 2021, p. 322-331.

fulfillment, service provision, etc. For instance, in providing express delivery services, it is necessary to obtain personal information such as the address and the recipient's name. However, if a merchant attempts to collect the user's height information, it is irrelevant to the fulfillment of the delivery service, meaning there is no necessity to collect it.M indicates appropriate importance, corresponding to general needs for personal information, such as collection for commercial purposes or data operations. For instance, when making clothing recommendations, collecting users' height and clothing size information is considered appropriate and in line with the ultimate purpose of the service. S indicates very important, primarily corresponding to special circumstances such as national security or legal requirements where obtaining personal information is necessary, with public interest taking precedence over individual rights. For instance, during the handling of acute infectious diseases, it is extremely necessary to collect data such as the patient's name, ID card, and past medical history. This not only concerns the individual's life safety but also holds significant value for public health security. Patients have the obligation to provide relevant information. Severe (S), moderate (M), and light (L) correspond to 2^2, 2^1, and 2^0, respectively.

W_i represents the importance of information in societal perception, which must be independently assessed based on the content of the personal information. It also has three levels: high (S), medium (M), and low (L). S represents extremely important information, such as personal information essential to basic human dignity or private information that should not be disclosed to others, for example, an individual's ID number. M denotes generally important information, which may pose a threat to personal information security but does not involve core rights, such as phone numbers or addresses. L denotes publicly available information that does not pose a threat to personal information security, typically information that cannot be used to identify an individual, such as randomly chosen online nicknames on a platform. W_j denotes the importance of obtaining information, determined independently based on social experience. It has three levels: severe (S), moderate (M), and mild (L). S denotes extremely important based on social experience, such as collecting personal information in cases involving national security or explicitly stipulated by law. M refers to general importance, which pertains to the collection and use of personal information in commercial operations, such as providing one's color and style preferences when purchasing goods. L refers to situations where the collection and use of personal information is not necessary, such as providing one's identity information when purchasing fruits, which is obviously excessive collection. The two parameters, high (S), medium (M), and low (L), correspond to 2^2, 2^1, and 2^0, respectively.

R refers to the reliability of the estimated experience. R_i refers to the probability of achieving P_i based on the estimated experience without interfering with P_j. This should be determined in specific usage scenarios, and the collection of information should be limited to what is necessary to achieve the intended purpose, with efforts made to minimize the collection of personal information. It should have two measures: moderate (M) and severe (S). M indicates that it is difficult to achieve the protection of personal information rights while not affecting the achievement of the intended purpose. For instance, without providing a home address, it is impossible to receive express delivery services, as judged by the general public. S indicates that the protection of personal information can be adequately achieved while meeting the intended purpose. For example, providing catering services without disclosing gender information. The numerical values for moderate (M) and severe (S) correspond to 2^0 and 2^1, respectively.

R_j represents the likelihood of achieving P_j without affecting P_i, indicating the ability to achieve the purpose of use without compromising personal information security. It also has two scales: moderate (M) and severe (S). M indicates difficulty in achieving the purpose of use without compromising personal information security,

such as realizing express delivery services without providing detailed addresses. S indicates the ability to achieve the purpose of use while adequately protecting personal information rights. For instance, a simple supermarket shopping transaction does not require the collection of any personal information. Moderate (M) and severe (S) correspond to 2^0 and 2^1, respectively.

"Entropy weight" is an effective quantitative indicator for measuring the ability of information recognition and "association", which can be specifically calculated in information systems and provide precise reference standards for parameter values such as Ii, Ri, and Rj. Information entropy and weighted formulas, as methods for evaluating the balance of personal information rights, can be used as specific means to judge the balance of interests among all parties in judicial practice, and also provide design references for the institutional framework of rights balance in the circulation of personal information.

"Information entropy" serves as an effective quantitative measure of information's identification and "association" capabilities, enabling specific numerical calculations within information systems and providing precise reference standards for parameter values such as I_i, R_i, and R_j. Information entropy and the weighting formula, as methods for assessing the balance of personal information rights, can serve as concrete approaches for judging the balance of interests among parties in judicial practice and as design standards for institutional frameworks ensuring rights balance in the circulation of personal information.

This article takes the entropy weight model constructed in the previous text as a sample, and simulates the data situation between information processors and individuals through information systems and specific information attribution states. Then, it brings objective usage scenarios into the weight formula to obtain a value judgment on the balance between an individual's information protection and the rights and interests of data flow circulation, including: commercial usage scenarios, Public safety demand scenarios, and social survey and interview scenarios.

As shown in Table 6, in the commercial usage scenario, information is collected and the balance between personal information rights and data flow is judged based on gender and education level. Ij and Wj are fixed values of 2^1 and 2^1 respectively. The amount of uncertainty eliminated from the information, Ii, is then determined, and the importance of the information, Wi, is independently judged based on experience and information entropy parameters. In this scenario, the entropy weight sum of the two types of information is 0.706, which can eliminate the vast majority of uncertainty. Ii is 2^1 and Wi is 2^2. Ri represents the possibility of protecting sensitive personal information without affecting business operations. Since most commercial operations only require basic information and do not need sensitive personal information, Ri is 2^1. Rj represents the possibility of achieving business goals without infringing on personal sensitive information, which is usually feasible, so Rj is 2^1. Substituting these values into the formula yields Wij = 2, which is greater than 1. The conclusion is that personal information rights should be given priority and the scope of personal information of information processors should be restricted.

Table 6. The value judgment of collecting Gender and Education Level for commercial use.

Usage scenarios and information collection content	**Parameter**	**Numerical value**	**Conclusion**
commercial usage: Gender+Education Level	I_i	2^1	2: personal information rights should be given priority
	I_j	2^1	
	W_i	2^2	
	W_j	2^1	
	R_i	2^1	
	R_j	2^1	

As shown in Table 7. In public safety demand scenarios, collect information and determine the balance between personal information rights and data flow circulation regarding gender, education level, birth month, and age. Ij represents the importance

of Pj, that is, the significance of obtaining personal information for the other party, reflecting the necessity of identifying the individual, which is 2^0. Wj represents the importance of obtaining information, which is 2^2. Continue to determine the amount of uncertainty eliminated from the information Ii, and independently judge the importance of information Wi based on experience and information entropy parameters. In this scenario, the entropy weight of the information is 1, which can completely eliminate uncertainty in identifying individuals, with Ii being 2^1 and Wi being 2^2. Ri represents the possibility of protecting sensitive personal information under public safety, which is 2^0. Rj represents achieving public safety without infringing on personal sensitive information, which is usually impossible, so Rj is 2^0. Substitute these values into the formula to obtain Wij = 1/2. The conclusion is that public safety is more important and should be given priority.

Table 7. In the Public Safety Usage, collect the value judgments of Gender, Education Level, Birth Month and Age.

Usage scenarios and information collection content	**Parameter**	**Numerical value**	**Conclusion**
Public safety usage: Gender+Education Level+Birth Month+Age	I_i	2^1	1/2: Public safety should be given top priority.
	I_j	2^2	
	W_i	2^2	
	W_j	2^2	
	R_i	2^0	
	R_j	2^0	

As shown in Table 8, in social survey and interview scenarios, information is collected and the balance between personal information rights and data flow is judged for Gender, Education Level, Birth Month and Age. Ij represents the importance of Pj, that is, the importance of obtaining personal information to the other party, reflecting the necessity of identifying individuals, which is 2^1. Wj represents the importance of obtaining information, which is 2^1. Continue to determine the amount of uncertainty eliminated from the information Ii, and independently judge the importance of the information Wi based on experience and information entropy parameters. In this scenario, the entropy weight of the information is 1, which can completely eliminate the uncertainty of identifying individuals, with Ii being 2^1 and Wi being 2^1. Ri represents the possibility of protecting sensitive personal information under public safety, which is 2^0. Rj represents achieving public safety without infringing on personal sensitive information, which is usually impossible, so Rj is 2^0. Substitute these values into the formula to obtain Wij = 1. The conclusion is achieving a balance between personal information protection and data flow.

Table 8. In social survey and interview usage, collect the value judgments of Birth Month and Age.

Usage scenarios and information collection content	**Parameter**	**Numerical value**	**Conclusion**
social survey and interview usage: Birth Month+Age	I_i	2^1	1: Achieving a balance between personal information protection and data flow.
	I_j	2^1	
	W_i	2^1	
	W_j	2^1	
	R_i	2^0	
	R_j	2^0	

4. Conclusion

The main challenges faced by the personal information protection system lie in clarifying the identification and association capabilities of personal information and balancing the rights of personal information with the interests in data flow. The "entropy weight model" can objectively express the "identification" and "association" capabilities of personal information and provide specific quantitative parameters for defining personal information. By applying Alexy's weighting formula to find the

balance point between rights and interests, the priority order of protection can be determined. In specific application scenarios, the use of the entropy weight model and Alexy's weighting formula can, based on objective parameters, judge and construct the priority order of the balance of rights and interests between personal information protection and data flow. This paper attempts to construct such a research paradigm. This effective personal information protection framework has good technical compatibility and can eliminate the interference of subjective factors, which is conducive to better constructing the balance of rights and interests in judicial practice, better protecting personal information, and promoting the efficient circulation and realization of interests in data flow.

5. Funding

This research was funded by the Shanxi Province 2024 Graduate Education Innovation Program, grant number 2024SJ004.

6. Data Availability Statement

The data that support the findings of this study are available from the corresponding author upon reasonable request.

7. Competing interest

The authors have no relevant financial or non-financial interests to disclose.

8. References

ACQUISTI, A. "The economics of personal data and the economics of privacy." Economics, v. 11, 2010, p. 24.

ACQUISTI, A.; TAYLOR, C.; WAGMAN, L. "The economics of privacy." Journal of Economic Literature, v. 54, n. 2, 2016, p. 442-492.

ALEXY, R. "The weight formula." *In Rights: Concepts and Contexts;* Routledge, 2017. pp. 539–558.

BEESLEY, S.J., POWELL, A., GROAT, D., BUTLER, J., HOPKINS, R.O., ROZENBLUM, R., BROWN, S.M. "Evaluating the balance between privacy and access in digital information sharing." *Critical Care Medicine,* v. 50, n. 2, 2022, p. e109-e116.

BERRESHEIM, L. Balancing Privacy and Other Rights. Doctoral dissertation, University of Amsterdam, Amsterdam, 2024.

CHENG, X. "Understanding and Application of Personal Information Protection Law." *China Legal Publishing House*, Beijing, China,2021.

CHEN, L., HUANG, Y., OUYANG, S., XIONG, W. *The Data Privacy Paradox and Digital Demand (No. w28854);* National Bureau of Economic Research, Cambridge, MA, USA, 2021.

CHESNOKOVA, L. V. "Information privacy: protecting freedom and individual autonomy." *The Digital Scholar Philosopher s Lab*, v. 4, n. 2, 2021, p. 145-157.

CLOAREC, J., MEYER-WAARDEN, L., MUNZEL, A. "Transformative privacy calculus: Conceptualizing the personalization-privacy paradox on social media." *Psychology & Marketing*, v. 41, n. 7, 2024, p. 1574–1596.

Ding, X. "On the Uncertainty of the Concept of Personal Information and Its Legal Responses." *Journal of Comparative Legal Studies*, v. 183, n. 5, p. 46-60.

FAINMESSER, I.P., GALEOTTI, A., MOMOT, R. "Digital privacy." *Management Science,* v. 69, n. 6, 2023, p. 3157-3173.

HARPER, J. "Personal Information is Property." SSRN Electronic Journal, 2024.

HE, B. "On the Definition of Personal Information Concept." *Information Communication Technology and Policy,* 2018, n. 6, p. 38-42.

KANG, J. "Information privacy in cyberspace transactions." *Stanford Law Review,* v. 50, n. 1, 1997, p. 1193-1254.

KORGANBEKOVA, M., ZUBER, C. "Balancing user privacy and personalization." *Work in Progress*, 2023, 6.

LAH, F. "Are IP addresses personally identifiable information?" *ISJLP*, v. 4, n. 3, 2008, p. 681.

NEKIT, K. "The (im)possibility of personal and industrial (machine-generated) data to be subject to property rights." *International Journal of Law and Information Technology*, v. 32, 2024.

NISSENBAUM, H. "Privacy as contextual integrity." *Washington Law Review*, v. 79, n. 119, 2004, p. 119-157.

LI, Q., JIANG, T., & FAN, X. "Examining Sensitive Personal Information Protection in China: Framework, Obstacles, and Solutions." *Information & Culture*, v. 58, n. 3, 2023, p. 247-273.

NOVELLI, C.; CASOLARI, F.; ROTOLO, A.; TADDEO, M.; FLORIDI, L. "AI risk assessment: a scenario-based, proportional methodology for the AI act." *Digital Society,* v. 3, n. 1, 2024, p. 13.

POPOWICZ–PAZDEJ, A. "The proportionality principle in privacy and data protection law." *Journal of Data Protection & Privacy,* v. 4, n. 3, 2021, p. 322-331.

POSNER, R.A. "The economics of privacy." *The American Economic Review,* v. 71, n. 2, 1981, p. 405-409.

PURTOVA, N. "From Knowing by Name to Targeting: The Meaning of Identification under the GDPR." *International Data Privacy Law,* v. 12, n. 3, 2022, p. 163-183.

SHANNON, C.E. "The mathematical theory of communication." *The Bell System Technical Journal*, v. 27, n. 3, 1948, p. 379-423.

SMITH, H.J., Dinev, T., Xu, H. "Information privacy research: An interdisciplinary review." *MIS Quarterly*, v. 35, n. 4, 2011, 989-1015.

TALAPINA, E. "The Right to Informational Self-Determination: On the Edge of Public and Private." *Legal Issues in the Digital Age*, v. 3, n. 4, 2022, p. 34-51.

TANG, J.; LUO, X.; CHEN, J.; YUAN, Y.; LOO, J. "An ethical decision making algorithm for autonomous vehicles during an inevitable collision." *In Proceedings of the 2024 4th International Conference on Big Data, Artificial Intelligence and Risk Management*, 2024, p. 1077-1081.

VOLD, K., & WHITTLESTONE, J. "Privacy, Autonomy, and Personalised Targeting: Rethinking How Personal Data Is Used." In Data, Privacy, and the Individual in the Digital Age, 2019.

WACHTER, S. "Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR." *Computer Law & Security Review*, v. 34, n. 3, 2018, p. 436-449.

XIAO, X. "An analysis and construction of personal information rights." *Chinese Journal of Law*, v.45, n. 6, 2023, p. 73.

XU, M. "Privacy Crisis and Tort Law Response in the Era of Big Data." *China Legal Science*, v. 2017, n. 1, p.130-149.