Technical Implementation Framework of AI Governance Policies for Cross-Modal Privacy Protection

Yuxiao Lei[1], Yucong Duan[1(✉)], and Mengmeng Song[2]

[1] School of Computer Science and Cyberspace Security, Hainan University, Haikou, China
duanyucong@hotmail.com
[2] School of Tourism, Hainan University, Haikou, China

Abstract. AI governance has been increasingly preeminent in digital world which presents a practical challenge of combining technical digital implementation with legal governance in real world. This work proposes a strategical bridging framework between AI governance policies and technologies on the fundamental content expression modals of data, information and knowledge, and crossing modals processing of DIKW content/resources through formalization abstract or intangible policies and their interactions as concrete technical tangible executions of modal transformations, essential computation and reasoning. The essential content oriented formalization, computation and reasoning of features, policies and associations bridging legal pursue and technical details is unified based our proposed existence computation and relationship defined everything of semantics mechanisms, which we further proposed as essence computation and reasoning for multiple modal and cross modal content. We demonstrate the feasibility and effectiveness of our essential content oriented multiple modals analysis and modeling through construction of a systemic privacy protection framework in the background of the whole process of perception, storage, transition and processing of user generated content in virtual communities. This solution framework seamlessly integrates originally discrete policies and demands on fairness, personal security, financial security, peace and quiet, autonomy, integrity against commodification and reputation at the technical execution level in terms of specific activities and concrete actions inside and cross data modal, information modal and knowledge modal.

Keywords: DIKW graph · Virtual community · Privacy protection · Right to privacy · Value of privacy

Supported by Natural Science Foundation of China Project (No. 61662021 and No. 72062015), Hainan Provincial Natural Science Foundation Project No. 620RC561, Hainan Education Department Project No. Hnky2019-13 and Hainan University Educational Reform Research Project No. HDJWJG03.

H. Gao et al. (Eds.): CollaborateCom 2020, LNICST 350, pp. 431–443, 2021.
https://doi.org/10.1007/978-3-030-67540-0_27

1 Introduction

The automated decision-making of artificial intelligence system is fast and convenient than, When the decision is related to people, it may lead to prejudice and discrimination against human individuals [1] and privacy violations [2].

The definition of privacy is related to human pensonal values. Nowadays, more and more users choose to share life in virtual community, or communicate with people with the same interest in data, information, knowledge and other forms of content. As a result, Virtual trace ($T_{virtual}$) left by users' browsing and User-generated content (UGC) posted by users themselves on virtual community are also included in the category of privacy. $T_{virtual}$ can reflect the user's own character and behavior [3], UGC can reflect the private resources of user which are not influenced by the outside world [4].

$T_{virtual}$ includes user browsing history, purchase history, and interaction history, and UGC includes text, video, voice and any other types of content that users post in virtual community. There exists a connection between Tvirtual and UGC that $T_{virtual}$ includes the behavior of users posting UGC.

A study on the privacy status of personal online social networks in the 10 most visited online social networking sites (OSNs) in the world indicated that many users ignore the privacy risks on OSN, and traditional privacy protection methods have limited effects on the protection of personal privacy [5]. In the four links of the circulation of private resources: Sensing, Storage, Transfer and Processing, The development of privacy protection technology lags behind the development of privacy acquisition technology. It's necessary for both virtual community and users to strengthen their awareness of privacy protection.

There are three parties involved in the circulation of privacy resources: Generator (User), Acquirer (Visitor) and Communicator (Virtual Community). The different party have different rights to privacy in the different links of circulation. The interaction and balance between the rights to privacy of the three parties combined with DIKW graph technology to maximize privacy protection. DIKW graph is a multi-layered architecture for processing typed resources, which can be divided into four parts: Data graph, Information graph, Knowledge graph and Wisdom graph. The DIKW graph technology can be used to optimize the processing efficiency of the integration of storage, transmission and calculation [6] and privacy data protection [7].

2 Privacy Resources of Users in Virtual Community

The privacy resource ($Privacy_{DIK}$, P_{DIK}) can be extracted from the $T_{virtual}$ and UGC in virtual community. Through the semantic formalization of key elements of P_{DIK} [8], P_{DIK} is classified into three types: $Data_{DIK}$, $Information_{DIK}$ and $Knowledge_{DIK}$, according to the differences of P_{DIK}'s own attributes, such as Eq. (1). All of the P_{DIK} represents a feature of users that can be used to analyze and define users.

$$Privacy_{DIK} = \{Data_{DIK}, Information_{DIK}, Knowledge_{DIK}\} \tag{1}$$

2.1 Privacy Resources in the DIKW Graph

Data, Information and Knowledge

$Data_{DIK}$. $Data_{DIK}$ is a directly observed discrete element that has no meaning without context and is not associated with a specific human purpose. In this paper, $Data_{DIK}$ refers to the attributes of the UGC that the user posts in virtual community, such as a photo, a paragraph of text, and the user's profile, name, age, degree, and so on.

$Information_{DIK}$. $Information_{DIK}$ or I_{DIK} is used to explore, analyze, and express the interaction between two entities, which can be either a person or other objects. In virtual community, I_{DIK} records the relationship $R(User, E_{associated})$ between users and entity directly connected to users, as well as the relationship $R(E, E_{other})$ between a entity and other entities. Relationships can define everything at the semantic level [9].

$Knowledge_{DIK}$. $Knowledge_{DIK}$ or K_{DIK} is derived from D_{DIK} and I_{DIK} through structural and formal derivation, and is further improved on the basis of I_{DIK}. I_{DIK} represents the relationship between individual entities. K_{DIK} summarized the relationship between entities of the same type on the basis of I_{DIK}.

K_{DIK} is the reasult of a induction and prediction of individual behaviors. K_{DIK} has two basic: the validity probability of $K_{DIK}(K_{DIK}(Val))$ and the precision probability of $K_{DIK}(K_{DIK}(Pre))$. $K_{DIK}(Val)$ refers to the probability of K_{DIK} predicting user behavior and psychology successfully. $K_{DIK}(Pre)$ indicates the abundance of related content contained in K_{DIK} for the same event. For example, $K_{DIK2}(Pre)$ is greater than $K_{DIK1}(Pre)$ as followed:

K_{DIK1} = "The user need Commodity_A"

K_{DIK2} = "The user need Commodity_A at Time_B"

Properties of Privacy Resource. In the case of two or more private resource contents with logical conflicts exists in DIKW graph. For example, virtual communities provide users with an environment separated from reality, in which users may create a virtual image that does not conform to their own real image. The $T_{virtual}$ and UGC is partly in line with the user's actual self image, and partly in line with the virtual image that users imagine in their minds.

As shown in Eq. (2), P_{DIK} are classified into $P_{consistent}$ and $P_{inconsistent}$ after traversal comparison with other P_{DIK}. If the result is ture, the $P_{consistent}$ belongs to $P_{inconsistent}$, which has no logical conflict with other P_{DIK}. If the result is false, the combination of P_{DIK1} and the conflict P_{DIK2} $P_{consistent}$ belongs to $P_{inconsistent}$, And there is logical conflict between the P_{DIK} in $P_{inconsistent}$.

$$TraverseCompare(P_{DIK1}, P_{DIK}) = \begin{cases} TURE \rightarrow P_{DIK1} \in P_{consistent} \\ FALSE \rightarrow (P_{DIK1}, P_{DIK2}) \in P_{inconsistent} \end{cases} \quad (2)$$

Group Privacy and Intimacy Group. P_{DIK} is not only belong to individuals, but also can belong to group. It is possible to dig out the P_{DIK} of individual's family members, friends, neighbors, and other groups based on the P_{DIK} of individuals.

Group privacy [10] exists in two or more entities E_1, E_2, ,E_n, which can be classified into Group relationship privacy ($GP_{relation}$) and Group content privacy ($GP_{content}$) according to their attributes. Entities in Group privacy constitute an intimate group ($G_{Intimacy}$) of mutual protection of privacy.$G_{Intimacy}$ is not limited to a collection of multiple individuals who are related, but can also be people of the same race, gender and age.

$GP_{relation}$ is the retention of R, which is the relationship between multiple entities. Users do not want to be known about their relationships with other users in $G_{Intimacy}$ by others; or for some purpose, not to be known by others. $GP_{content}$ refers to the P_{DIK} shared by $G_{Intimacy}$, in which the importance of different individuals on P_{DIK} may vary due to individual differences but remain within a certain range.

2.2 Handle of Privacy Resources

There are a lot of duplicate and invalid P_{DIK} in virtual community. It is necessary to organize P_{DIK}K before DIKW graph modeled, which includes extract, transform and load (ETL), transferring P_{DIK} from virtual community as a source to the destination of the DIKW graph.

Extraction of Privacy Resources. The extraction of P_{DIK} includes extracting the content of P_{DIK} from homogeneous or heterogeneous source. Based on the self-subjectivity of privacy, different users have different reservation degree of P_{DIK}, and the standards of P_{DIK} extraction are different.

Users have different degrees of reservation to different $P_{DIK}(D_{Res})$. The higher the value of $P_{DIK}(D_{Res})$, the higher the retention of P_{DIK}. When the value of $P_{DIK}(D_{Res})$ is higher than the threshold D_W, the P_{DIK} is classified $Secret_{DIK}$ as shown in Eq. (5), which and will be abandoned in the process of extracting P_{DIK}.

$$Secret_{DIK} = \{P_{DIK} | P_{DIK}(D_{Res}) > D_W\} \tag{3}$$

As shown in Eq. (4), the function Reserve is constructed to calculated $P_{DIK}(D_{Res})$ based on the source of P_{DIK} ($P_{DIK}(Source)$) and the behavior record group associated with the P_{DIK} ($Inter(P_{DIK})$) which storaged in $InformationGraph_{DIK}$.

$$P_{DIK}(D_{Res}) = Reserve(P_{DIK}(Source), Inter(P_{DIK})) \tag{4}$$

Among them, $P_{DIK}(Source)$ includes $T_{virtual}$ and UGC, and $T_{virtual}$ belongs to passive resources, UGC belongs to active resources. In general, the $P_{DIK}(D_{Res})$ of P_{DIK} from $T_{virtual}$ is higher than P_{DIK} from UGC.

$Inter(P_{DIK})$ includes positive behavior $Inter^{pos}$ and negative behavior $Inter^{neg}$ in the protect of P_{DIK}, which are respectively positively and negatively correlated with the value of $P_{DIK}(D_{Res})$.

Transition of Privacy Resources. P_{DIK} can be converted by the Transition module to a new privacy resource (${P_{DIK}}^{new}$). There are three kinds of transition, First-order Transition, Multi-order Transition and Technical Transition in Transition module.

$P_{DIK}(In)$ denote the degree of entry of each P_{DIK}, which is the degree generated by the other P_{DIK}. $P_{DIK}(Out)$ denote the degree of exit of each P_{DIK}, which is the way generated by the other P_{DIK}.

First-order Transition. First-order Transition to generate a new ${P_{DIK}}^{new}$ from a single P_{DIK}, Which includes same-type transition and cross-type transition among D_{DIK}, I_{DIK} and K_{DIK}.

Multi-order Transition. Multi-order Transition is also known as Associative Transition, refer to generating ${P_{DIK}}^{new}$ by combining several P_{DIK}. There is no limit to the type and number of P_{DIK} and ${P_{DIK}}^{new}$ in a Multi-order transition.

${P_{DIK}}^{(1)}$ represents an initial P_{DIK}; ${P_{DIK}}^{(2)}$ represents a P_{DIK} connected to ${P_{DIK}}^{(1)}$; ${P_{DIK}}^{3}$ represents a new ${P_{DIK}}^{new}$ generated by combining ${P_{DIK}}^{(1)}$ with one or more ${P_{DIK}}^{(2)}$.

Technical Transition. First-order and Multi-order Transition are simple P_{DIK} transition based on common sense reasoning, while other P_{DIK} transition require the assistance of technology and other resource contents, which is Technical Transition. Technical transition of P_{DIK} has different difficulty, and is not necessarily able to complete. The difficulty of Technical transition is related to the entity E involved in the transition. As shown in Eq. (5), the function Difficulty is constructed to compute the difficulty of transitioning P_{DIK} to a ${P_{DIK}}^{new}$ ($T_{Difficulty}$). The content of E includes the technology(E_{tech}) and other resources ($E_{resource}$). When the $T_{Difficulty}$ is infinite, it means that P_{DIK} can not be transitioned to ${P_{DIK}}^{new}$ with only entity E.

$$\begin{aligned} T_{Difficulty} &= Difficulty(P_{DIK}, {P_{DIK}}^{new}, E) \\ &= Difficulty(P_{DIK}, {P_{DIK}}^{new}, E_{tech}, E_{resource}) \end{aligned} \tag{5}$$

Load of Privacy Resources. Load of P_{DIK} means insert P_{DIK} into final target storage medium. After extraction and transition, the DIKW graph will be modeled based on all P_{DIK} by classifying P_{DIK} into D_{DIK}, I_{DIK}, K_{DIK} and storaged separately on Data graph, Information graph, Knowledge graph, which constitute DIKW graph of user [11], such as Eq. (6).

$$DIKWGraph = \{DataGraph, InformationGraph, KnowledgeGraph\} \tag{6}$$

In addition, load of P_{DIK} also includes the modeling of the group DIKW graph shown in Eq. (7), which taking $G_{Intimacy}$ as a entity E and $GP_{content}$ of $G_{Intimacy}$ as P_{DIK}. There exists relation between $DIKWGraph^G$ and the *DIKWGraph* of the user in $G_{Intimacy}$ but is reserved as $GP_{relation}$. And the realtion between individuals of $G_{Intimacy}$ is also reserved as $GP_{relation}$. $GP_{relation}$ is stored in $InformationGraph^G$.

$$DIKWGraph^G = \left\{ DataGraph^G, InformationGraph^G, KnowledgeGraph^G \right\} \quad (7)$$

2.3 The Value of Privacy

Privacy is a big category, in a narrow sense, it includes the individual's control of self-resources. In a broad sense, it represents many different interests and values, including fairness, personal security, financial security, peace and quiet, autonomy, integrity against commodification and reputation.

Fairness. In the automated decision-making of AI system, different individuals should be treated fairly. Privacy protection is an important part of ensuring fairness of decision-making of AI system.

Such as Eq. (8), the function Fairness is constructed to compute fair index $V_{Fairness}$ of AI system. $V_{Fairness}$ is true means the decision-making of AI system meet the need for fairness and is legal.

$$V_{Fairness} = Fairness(P_{DIK(G)}, U_{price}) \quad (8)$$

Where $P_{DIK(G)}$ represents the group of P_{DIK} participating in decision-making of AI system that should not include any P_{DIK} will affect the decision-making. U_{price} represents the price that different individuals need to pay. For example, the U_{price} of normal people and people with disabilities in the same event is different. Therefore the AI system should try to balance the costs of the two through additional conditions when making relevant decisions to ensure the fairness for everyone.

In addition, the AI system should also be equipped with an additional "application-verification-approval" mechanism to correct decision errors caused by the untimely update of DIKW graph.

Personal Security. P_{DIK} related to personal security of user includes travel trajectory, home address, commuting time and so on. The leakage of P_{DIK} will increase the possibility of users being attacked by potential attackers.

As shown in Eq. (9), the function PS as followed is used to calculate the personal security index V_{PS}. When V_{PS} is higher than the threshold ${V_{PS}}^W$, it is proved that the personal safety of the user can be guaranteed and the decision behavior of AI system is leagal.

$$V_{PS} = PS(E, P_{DIK(G)}) \quad (9)$$

Where the visiting entity E includes the purpose of E ($E_{purpose}$) and the indentity of E (E_{ID}). It is part of the decision-making work of AI system to verify the identity of the visitor and determine the $P_{DIK(G)}$ transmitted to the visitor based on ($E_{purpose}$).

Financial Security. In the process of financial security protection, different from personal security, the AI system not only need to verify the identity of the visitor, but also need to consider the group privacy attributes of financial security. The target of harcker that can threatens the security of property is not a specific user, but the user with the most property in a $G_{Intimacy}$.

When two $G_{Intimacy}$ contain the same user, the privacy disclosure of $G_{Intimacy1}$ will affect the privacy protection of $G_{Intimacy2}$. For example, the attacker can infers the rich gathering area based on the home address of the user with the highest assets in $G_{Intimacy1}$, which will affect the financial security of $G_{Intimacy2}$ composed of the user and his neighbors.

As shown in Eq. (10), the function FS is constructed to calculates the financial security index (V_{FS}) of user. When V_{FS} is higher than the threshold ${V_{FS}}^{W}$, the financial security of user in the decision-making process of AI system can be guaranteed, and the decision-making behavior of AI system is legal.

$$V_{FS} = FS(E, P_{DIK(G)}, GP_{content}) \tag{10}$$

Peace and Quiet. In the virtual community, many users maintain a virtual image which is different from own real image in the real world, and trying to keep it that way. In the virtual community, many users maintain a virtual image that is different from the real image in the real world, and want to maintain this state without being disturbed. Users do not want others in the virtual community to know their identities in the real world, nor do they want contacts in real life to know their ID numbers in the virtual world. The existence of the virtual community provides a "window" for many users to escape from the real world. When privacy is protected, Virtual communities can give users a state of peace and quiet that they want but can not have in the real world.

The mutually exclusive privacy resource group $P_{inconsistent}$ is a conflict created by a user's desire for two different identities. As shown in Eq. (11), The function PQ is constructed to calculate V_{PQ} based on $P_{inconsistent}$ When V_{PQ} is higher than the threshold ${V_{PQ}}^{W}$, The dual identity of user will not be disturbed and the decision-making of AI system is legal.

$$V_{PQ} = PQ(P_{inconsistent}, P_{DIK(G)}) \tag{11}$$

Autonomy. Autonomy means that individuals are free and able to act and choose and do what they want. Privacy and autonomy are important to individual growth. Nowadays, with the development of big data technology, the problem of "technology crossing the boundary" has arisen in the collection and use of individual P_{DIK}, which infringes the autonomy of users.

The recommend system is an important part of AI system. The recommend system provides users with appropriate customized services based on $Knowledge_{DIK}$ of users, but the customized services should not be limited to the most suitable for the user calculated by the AI system. While using big data technology, the user's right to choose autonomously should be guaranteed.

The success rate of recommend($R_{recommend}$) to user of AI system can reflect the user's acceptance of the recommend system. As in Eq. (12) , the function Autonomy is constructed to calculate the autonomy index $V_{Autonomy}$. The AI system will recommend different lines to different users according to $V_{Autonomy}$.

$$V_{Autonomy} = Autonomy(R_{recommend}) \tag{12}$$

Integrity Against Commodification. Commodification refers to the behavior that treat individual, life or human nature as a pure commodity which puts money above personal life. Privacy protection is also a protection of the individual. The individual should not be treated differently because of age, race, education level or economic class in particular systems such as health care and law.

As shown in Eq. (13), the function IAC is constructed to calculate V_{IAC} in the decision-making process of AI system. If and only if V_{IAC} is true, the decision-making process conforms to the requirements of integrity against commodification, and the decision-making behavior is legal. Where $E_{purpose}$ represents the different decision-making system such as law system. V_{IAC} is calculated by comparing $E_{purpose}$ and $P_{DIK(G)}$.

$$V_{IAC} = IAC(E_{purpose}, P_{DIK(G)}) \tag{13}$$

Reputation. Reputation is closely related to privacy, and the defamation of others is an invasion of privacy. Defamation refers to make an incorrect characterization or association of user based on true or false P_{DIK}, so that the reputation or psychological, emotional health of user are affected.

Equation (14) is used to calculate the reputation index $V_{Reputation}$, If $V_{Reputation}$ is higher than ${V_{Reputation}}^{W}$, it means that the decision-making process of AI system will not affect the reputation of user, and the process is legal.

$${V_{Reputation}}^{W} = Reputation(E_{purpose}, E_{ID}, P_{DIK(G)}) \tag{14}$$

3 The Rights in Circulation of Privacy Resources

The circulation of privacy resources in decision-making process has four circulation links: Sensing, Storage, Transfer, and Processing. The rights to privacy in circulation includes the right to know, the right to participate, the right to forget and the right to supervise.

3.1 Rights to Privacy

Right to Know. The right to know refers to the individual's right to know and obtain P_{DIK}. The right to know is not unlimited but differentiated according to different participants.

The right to know includes *Know(course)* and *Know(content)*. *Know(course)* is the right to know about the circulation of P_{DIK}, including $Sensing^K$, $Storage^K$, $Transfer^K$, $Processing^K$. *Know(content)* is the $P_{DIK(G)}$ calculated in Eq. (15), which represents what the participant have the right to know(${P_{DIK(G)}}^{Know}$).

$$ {P_{DIK(G)}}^{Know} = Know(E_{ID}, E_{purpose}, process) \tag{15} $$

As shown in Eq. (15), ${P_{DIK(G)}}^{Know}$ is calculated based on the identity and purpose of participant. Besides, *Know(content)* of the same participant in different processes is also different.

Right to Participate. The right to participate refers to the right of the method participant participating in the management and decision-making of P_{DIK}. As shown in Eq. (16), the function Participate is constructed to calculate the content of right to participate(*Participation*), Such as the form of participating, the number of participating and the deadline of participating.

$$ Participation = Participate(E_{ID}, E_{purpose}, process) \tag{16} $$

Right to Forget. The right to forget refers to remove old P_{DIK} (${P_{DIK}}^{old}$) and unvalue P_{DIK} (${P_{DIK}}^{unvalue}$) from the DIKW graph. ${P_{DIK}}^{old}$ is the P_{DIK} that is replaced by a new P_{DIK} over time. ${P_{DIK}}^{unvalue}$ is the P_{DIK} whose value is less than the storage cost.

A forgetting period T_{forget} is set to prevent the influence of ${P_{DIK}}^{old}$ on decision-making of AI system and the drag of ${P_{DIK}}^{unvalue}$ on virtual community. Every period of T_{forget} is passed, the virtual community will take place a systematic forgetting of P_{DIK}.

Right to Supervise. The right to supervise in the process circulation of P_{DIK} can be divided into logic supervision(S_{logic}), value supervision(S_{value}) and right supervision S_{right}. The right of supervision is the threshold of the decision-making process of AI system, only the supervision result of each participant in each process is true, the decision-making behavior is legal. The subject of supervision can be any interested participant.

Logic Supervision. Logicl supervision is mainly to supervise the common basic logic errors. For example, the number of votes is greater than the number of voters, which a logic error occurred in the decision-making process. The result of S_{logic} is false and the decision-making result is legal and not recognized.

Value Supervision. There are seven values of privacy: fairness, personal security, financial security, peace and quiet, autonomy, integrity against commodificatione and reputation, which is the content needs supercised of value supervision. When $V_{Fairness}$ and V_{IAC} are true, and the others greater than their respective thresholds, S_{value} is true and the decision-making process of AI system is legal.

Right Supervision. Right supervision is to supervise whether the use of privacy rights by participants exceeds the limit in each process. S_{right} includes S_{know}, $S_{paticipate}$ and S_{forget} in all four links of circulation.

3.2 The Circulation of Private Resources

Sensing. The sensing process occurs between Generator and Communicator. Virtual communities extract P_{DIK} from $T_{virtual}$ and UGC, and model a DIKW graph of user based on P_{DIK}. The rights to privacy involved in the Sensing process are:$Know_G$, $Know_C$, $Participate_C$, $Supervise_{(G-C)}$, $Supervise_C$.

Storage. The storage process is that Communicator storage the DIKW graph of different types P_{DIK} in a medium that can be accessed and restored. Some of the privacy rights involved include: $Participate_C$, $Forget_C$, $Forget_G$, $Supervise_C$.

Transfer. Transfer is the process that Communicator transfers P_{DIK} on the DIKW graph to Acquirer. Some of the privacy rights involved include: $Know_A$, $Know_G$, $Participate_A$, $Supervise_{(C-A)}$, $Supervise_{(A-C)}$, $Supervise_{(G)}$. Among them, $Know_G$ and $Supervise_{(G)}$ are the inherent rights of user. In practice, it possible for user not to exercise their rights, but both of these rights still exist.

Processing. Processing is the process that Acquirer exploits and develops a P_{DIK} obtained from virtual community. The privacy rights involved are as follows: $Participate_A$, $Supervise_{(G-A)}$, $Supervise_A$.

4 Privacy Protection

The significance of privacy protection is to provide guidance that can reduce the privacy risk and enable the AI system to make effective decisions in resource allocation and system control.

The privacy protection has a three-layer decision mechanism. The first layer is the supervision mechanism, each participant has the right to supervise in the process of P_{DIK} circulation. The second layer of privacy protection is anonymous mechanism, which protects P_{DIK} generated by sigle P_{DIK}. The third layer is partition mechanism, which protects P_{DIK} generated by multiple P_{DIK}.

4.1 Anonymous Protection Mechanism

Data Anonymous Protection. Data anonymous protection can be used to protect particular $Data_{DIK}$. For example, a negative or positive HIV test result(D_{DIK1} = "HIV=negative/positive") is represented by the value of parameter A ($D_{DIK1}{}^{A}$ = "A = 0/1") in the trasfer process of P_{DIK}.

The professional visitor with eligible for access ($Visitor_{profession}, Visitor_{pro}$) has the ability to restore $D_{DIK1}{}^{A}$ back to D_{DIK1}. Whereas a Hacker who is not qualified to access D_{DIK1} does not have the ability even if he obtained $D_{DIK1}{}^{A}$ through improper means. Data anonymous protection can reduce the risk of P_{DIK} leakage at the data level.

Information Anonymous Protection. Information anonymous protection is to hide the relationship between user and other entities through anonymity. For example, as shown followed, $I_{DIK1}{}^{A}$ generated by I_{DIK1} after anonymization:

I_{DIK1} = "User A tested positive for HIV"
$I_{DIK1}{}^{A}$ = "User XX tested positive for HIV"

The anonymization of I_{DIK1} does not affect $Visitor_{pro}$ with medical research purposes to use of private resources of patient. But it's difficult for hacker to connect $I_{DIK1}{}^{A}$ with a specific user. Information anonymous protection contributes to reduce the risk of patient privacy leakage.

Knowledge Anonymous Protection. Knowledge Anonymous Protection is that the attribute $K_{DIK}(Val)$ of K_{DIK} is concealed. The K_{DIK} trasferred by by Communicator to Acquirer is a collection of all possible K_{DIK} rather than the most possible single K_{DIK}. The solution of target K_{DIK} based on the visitor's purpose will diverge to varying degrees, and the solution space of K_{DIK} will expand with multiple $K_{DIK1}{}^{A}$. The validity of all K_{DIK} is the same for visitor, and visitor will provide difference services based on different $K_{DIK}{}^{A}$, which can ensure choice autonomy of user.

4.2 Partition Protection Mechanism

It is known that the P_{DIK} on DIKW graph can be transformed to $P_{DIK}{}^{new}$. If the calculated $T_{Difficulty}$ of P_{DIK} according to Eq. (5) is infinite for visitor, the P_{DIK} will be allowed to transfer to Acquirer by Communicator. Beacause the visitor has no ability to transform P_{DIK}, and will not cause the threat of irrelevant P_{DIK} disclosure.

The decision to protect P_{DIK} based on $T_{Difficulty}$ does not apply to all situations, because in some cases the calculation of $T_{Difficulty}$ is too troublesome. If both P_{DIK} can meet the needs of visitor in decision-making of AI system, the P_{DIK} with a small $P_{DIK}(Out)$ will be choosen as output. The smaller the $P_{DIK}(Out)$, the smaller the possibility of P_{DIK} being transformed to $P_{DIK}{}^{new}$, and the smaller the risk of leakage of irrelevant P_{DIK}.

5 Conlusion

$T_{virtual}$ and UGC left by user in virtual community is kinds of privacy resources and can be classified into data resources, information resources and knowledge resources which constitute the DIKW graph. Then the protection of $T_{virtual}$ and UGC in the law is seriously lagging behind. The application of big data technology in and $T_{virtual}$ and UGC has created a "technology crossing the boundary" problem but neither the operators of the virtual community nor the users themselves are aware of this problem.

There are four links of circulation of privacy resources: Sensing, Storage, trasfer and processing. The four links are completed by one or two of the three participants: Generator (User), Communicator (Virtual community) and Acquirer (Visitor). A legal framework of AI Governance for privacy resources protection in virtual community is established by clarifying the content of rights to privacy of each participant in each link. The content includS the privacy allowed to be known, the form of participation, the time when private to be forgotten, and so on. And the supervision mechanism is used to ensure that participant does not exceed the scope of their privacy rights. In addition, anonymous and partition mechanisms have also been applied to the protection of private.

References

1. Bozdag, E.: Bias in algorithmic filtering and personalization. Ethics Inf. Technol. **15**(3), 209–227 (2013)
2. Mittelstadt, B., Allo, P., Taddeo, M., Wachter, S., Floridi, L.: Bias in algorithmic filtering and personalization. Ethics Inf. Technol. **15**(3), 209–227 (2016). https://doi.org/10.1007/s10676-013-9321-6
3. Girardin, F., Calabrese, F., Fiore, D., Ratti, C., Blat, J.: Digital footprinting: uncovering tourists with user-generated content. IEEE Pervasive Comput. **7**(4), 36–43 (2008)
4. Krumm, J., Davies, N., Narayanaswami, C.: User-generated content. IEEE Pervasive Comput. **7**(4), 10–11 (2008)
5. Ulrike, H.: Reviewing person's value of privacy of online social networking. Internet Res. **21**(4), 384–407 (2011)
6. Song, Z., et al.: Processing optimization of typed resources with synchronized storage and computation adaptation in fog computing. Wirel. Commun. Mob. Comput. **2018**, 3794175:1–3794175:13 (2018)
7. Duan, Y., Lu, Z., Zhou, Z., Sun, X., Wu, J.: Data privacy protection for edge computing of smart city in a DIKW architecture. Eng. Appl. Artif. Intell. **81**(MAY), 323–335 (2019)
8. Daries, J., et al.: Privacy, anonymity, and big data in the social sciences. IEEE Pervasive Comput. **57**(9), 56–63 (2014)
9. Duan, Y.: Towards a Periodic Table of conceptualization and Formalization on Concepts of State, Style, Structure, Pattern, Framework, Architecture, Service, etc. Based on Existence Computation and Relationship Defined Everything of Semantic. SNPD (2019)

10. Mittelstadt, B.: From individual to group privacy in big data analytics. Philos. Technol. **30**(4), 475–494 (2017). https://doi.org/10.1007/s13347-017-0253-7
11. Duan, Y., Sun, X., Che, H., Cao, C., Yang, X.: Modeling data, information and knowledge for security protection of hybrid IoT and edge resources. IEEE Access **7**, 99161–99176 (2019)