Webology, Volume 13, Number 1, June, 2016

| Home | Table of Contents | Titles & Subject Index | Authors Index |

Roles of information systems in socio-legal context

Xingan Li

Endowed Senior Research Fellow, Beihang University, China; Associate Professor, Tallinn University, School of Governance, Law and Society, Estonia.

E-mail: xingan.li (at) yahoo.com

Received April 29, 2016; Accepted June 25, 2016

Abstract

Contemporary conception of information has been studied for decades. Starting from legal viewpoint, purpose of this article is to provide methodological understanding of the conception and classification of information in the domain of law, and the challenge it poses to the traditional legal system. In this article, information is classified into five categories according to the value it has and by whom it is held: information with positive value, value-neutral information, valueless information, information with negative value, and information with disputable value in different communities. The article analyzes the legal gaps accompanied by the proliferation of information systems, i.e., the lag of a legal notion, the legislative gap, and the jurisdictional gap. There has not been adequate preparedness to respond to cybercrime. The process of recognition and acceptance requires much time. The imperative requirement is for people to be well informed about the loopholes the legal system has and how they can be altered.

Keywords

Information; Information systems; Law; Social order; Social control; Cyberspace; Cybersecurity; Cybercrime

Introduction

When we explore society, we begin with observing human beings ourselves. Human beings have a determination of orientation to survive and to front the uncertain, unstable and uncontrollable environments, both physical and social environments, whether natural, constructed or cyber (a theme developed based on Coleman, 1990). It is this orientation to survive the uncertainty and to know the unknown that propels human beings to reshape the already shaped, reconstruct the already constructed, and reorganize the already organized.

While the discussion here will not be reduced to philosophical assertion, I accept that change is the eternal attribute of society.[1] Accumulation of information contributes greatly to social transformation. Digital information has become the decisive innovative factor in economic development and the leading resource in contemporary civilization (Molitor 1982, p. 84; Fisher 1984, p. 1; Rabin and Jackowski (eds) 1988; Daler and co-workers 1989, p. 13). Just as good land is a decisive factor for the agrarian economy, capital for the industrial economy, existing knowledge is a decisive factor for the information economy (Stonier 1983, p. 21). The relationship between these factors is not simply parallel, but progressive. In contrast to land, capital and information are more closely linked to human interactions. In contrast to land and capital, information is more closely linked to interactions of human intelligence. To say their relationship is in a progressive style is to say that information is the newer and higher level of achievements of human efforts (See Table 1). The implication of the recent information revolution lies in the fact that it is designed to eliminate the shortage of knowledge by processing data and information.

Table 1. Land, Capital and Knowledge

Factors	Land	Capital	Knowledge
Forms of the economy	Agrarian	Industry	Information economy
Forms of interaction	Non-interaction	Human-human interaction	Human-machine-human interaction

Information is therefore the enormous wealth of the social progress, which has been considered the fourth resource (UNCJIN 1999, Paragraph 85), alongside natural resources, property resources, and human resources. In contrast to other resources, information can be regarded as the only resource that can really be shared (Stonier 1983, p. 19). Fisher used a metaphorical statement describing information as power, “power to manage, power to manipulate, power to control” (1984, p. 1). Tapscott, Ticoll and Lowy (2000) further discussed the conception of digital capital in terms of business, stating that digital capital emerged from the incorporation of three types of knowledge assets: human capital, customer capital, and structural capital (p. 5).

With the network, people could “gain human capital without owning it; customer capital for complex mutual relationships; and structural capital that builds wealth through new business models.” (ibid.)

Other scholars further put information into a dynamic wealth-creating process, regarding information (particularly knowledge) a “key wealth-creating assets” (Porter and Read 1998, p. 26) apparently in a dynamic productive and reproductive process. Information processing is thus a process of promoting social productivity.

Unquestionably, the traditional resources have been seen as incomparable with the capacity of information, which can bring about enormous productivity and unprecedented social transformation. Information and related technology has created a new epoch, a new society, and a new way of thinking for the modern human beings. In our reading of traditional society, one thing stands out as fundamentally different from the information society, which is information dependent, information abundant, and information shared. Bjørn-Anderson and co-workers (1982) correctly predicted that the information society would be characterized by the remarkable increase of information flow, the contraction of temporal and spatial constraints, the increasing dependence of social life on information systems, and the synchronous application of new technology on society (pp. xi-xii). It is apparent that people consider information as being of positive value and grant potential power in its conceptual category.

People usually distinguish information from both data and knowledge. According to Stonier (1983), data is a series of unconnected facts and observations, likely to be changed to information through refining or organizing activities, while knowledge is organized form of information, providing the basis for insight and judgments (p. 19) Detailed relations between the terms can be illustrated as in Figures 2 and 3. On the other hand, information at one level may merely be data at another level (ibid). Finally, there can never be a clear limit between these terms. They are usually used interchangeably. For example, knowledge is the highest level of data or information, but people do not talk about knowledge security instead of data security and information security. In addition, information systems are actually “data systems”,[2] but the favourite term in various disciplines is still “information systems”. In this study, the word “information” is priority choice where these three words can be used interchangeably.

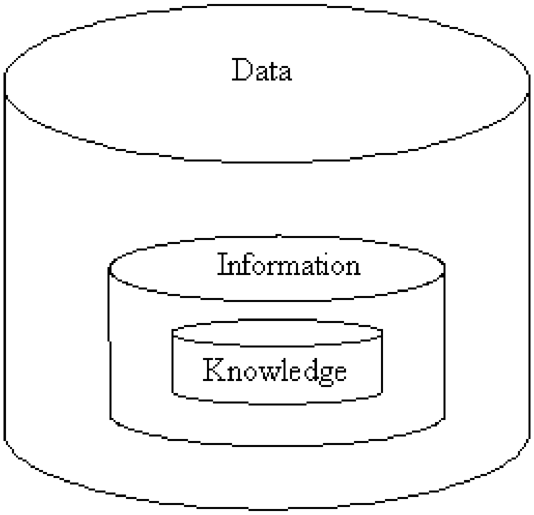

Figure 1. Relations between Data, Information and Knowledge

A proportion of data is information, from which a proportion is drawn as knowledge.

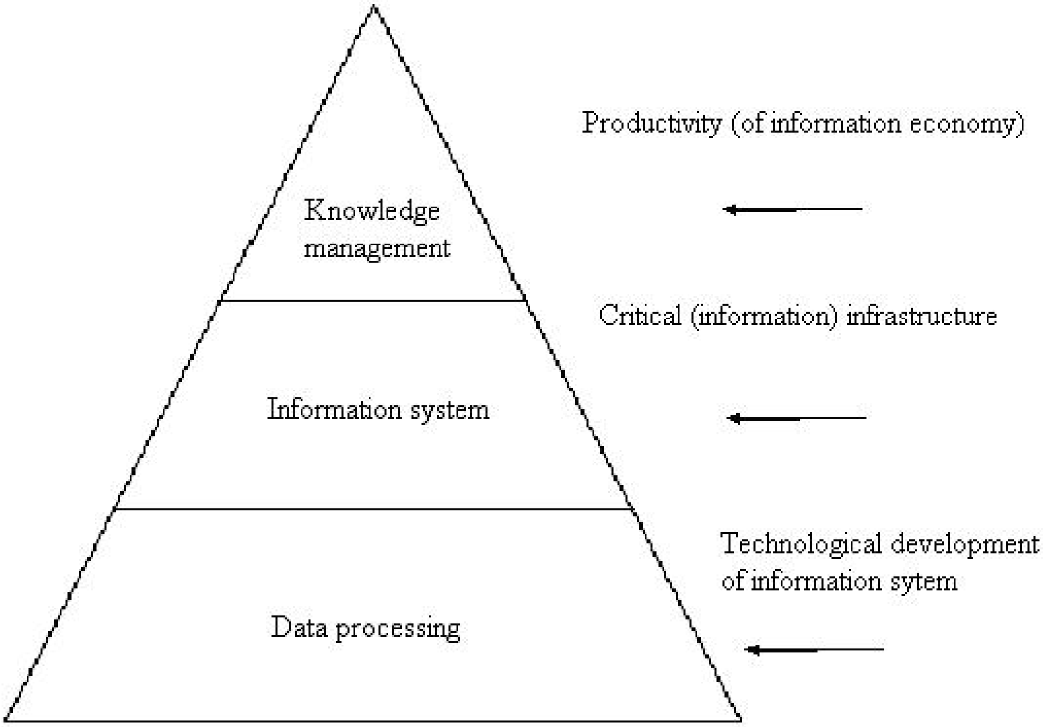
Knowledge management
Information system
Data processing
Productivity (of information economy)
Critical (information) infrastructure
Technological development of information sytem

Figure 2 . Social Roles of Data, Information and Knowledge

Data processing is achieved through technological development. Information systems are a part of critical infrastructure. Knowledge management is an element of productivity. The phrases in brackets denote the alternative usage of the terms when they are used interchangeably.

In sum, the strong and the wealthy in the agricultural society strive for more and better land; the strong and the wealthy in the industrial society strive for more and better capital; and the strong and the wealthy in the information society strive for more and better information.

Nevertheless, the term "information" is theoretically used as a value-neutral term. From the viewpoint of law, the term "information" stands for "data, text, images, sounds, mask works, or computer programmes", including the process of collecting and compiling them.[3] Important elements involved in defining information in the modern sense include:

Information is electronized. The current processing form of information is characterized by mobilization through electricity, fastest known vehicle. Information is digitalized. The current information is processed in the form of digits, "0" and "1". Information is computerized. Information is created, deposited, processed and transmitted by the assistance of computer, a powerful "information machine" (Konig 1967, p. 1).

Information is automatized. The process in which information is created, deposited, processed and transmitted is a kind of human-machine interaction. There is no absolute automitization. Information is networked. Information is transmitted through the networks. It is electricity, digits, computer and automitization that constitute the basis of the networks. Information is modernized. It is not in a process of modernization, but in a process from modern to post-modern. It is modernized thus transformed. The change breaks the equilibrium of the conventional control and organization, motivating somebody to harvest from deviant actions, exposing somebody else to potential threats, and reducing the effectiveness of any safeguard.

Information is evaluated. The value of information is recognized, accepted and respected. Lacking any of these elements, the object can hardly be regarded as information. The modern definition of information therefore inevitably contains different factors from the traditional meaning of this term. Many people nonetheless misunderstand the exact meaning of information and consider that law has regulated information for several centuries or millenniums. This suggestion ignores the difference between information in the traditional sense and that in the modern sense. While the traditional form of information is heavily substance dependent, the modern information is processed by digital technique. The present information is practically transformed into digital information, regardless of whether it ever existed in the pre-computer era. Particularly, on account of the specific form of existence, a copy of information is not necessarily different from the original information in content, quality and medium. Under such circumstances, the term "information" can precisely cover a copy of information.[4] In the network environment, information, its copies, and the copies' different digits may be transmitted along the cable, fibre, or wireless networks without the spatiotemporal limits.

The purpose of the article is to deal with the conception and classification of information in the domain of law, and the challenge it poses to the traditional legal system. Considering the different roles of different categories of information in the legal system, it is necessary to classify information according to its value from the standpoint of law. Law does not provide equal protection for all kinds of information. On the contrary, law merely encourages the processing of information with a positive value, but discourages the processing of information with a negative value. Although people deem information systems to be part of a critical infrastructure, and we transmit various kinds of information through the same information systems, the legal nature of these kinds of information should be differentiated.

Classification of information in the legal sense

Social inquiry usually starts from conceptualization (Babbie, 1995). Having talked about the conception of information, and not necessarily repeating accepted definitions, this section will give a sketch of classification.

The legal value of information has long been recognized.[5] The legal effect, validity or enforceability of information should not be rejected simply on the ground that it is in a form different from that seen in traditional documents.[6] As in United States v. Adajan case the court ruled that computers could be at the same time storerooms of private information that must be guarded, or that of criminal proofs that must be identified.[7]

Previously, people were inclined to dichotomize information into legitimate and illegitimate, for instance, Sterling (1994). The nature and content of information are far broader than merely being legitimate and illegitimate. The value of information can be regarded as a criterion for a typology. On this terrain, information can be sorted into five categories according to the value it has and by whom it is held: information with positive value, value-neutral information, valueless information, information with negative value, and information with disputable value in different communities.

The first category of information, information with positive value has the capacity to promote social welfare. The positive value of this category of information depends on the content of the information. If the offenders access to or destroy such information without authorization, the value of that information would be abused or exterminated. Loss of information with positive value, or loss of value of such information, either due to breach of its confidentiality, integrity, or availability, diminishes the efficiency of the information owner or, in turn, promotes the efficiency of the opponent. Offences involving infringement of information with positive value, infringe the rights and interests of the information owners. The related acts include unauthorized acquisition, modification of, destruction of, and tampering with information, and interference with information transmission. In particular, offences related to the ownership of information may possibly infringe the rights to information, such as appropriation, unauthorized use, obtaining income, and disposition. To copy, retrieve, deposit, publish, duplicate, utilize, promulgate, transmit, conceal, encrypt, decrypt, transfer, sell, etc., without authorization or legal permission, are all conducts that can breach the ownership of information.

The second category of information, value-neutral information indicates that the value of information cannot be classified into positive or negative. Rather, it can be utilized as either positive information or negative information, or used as positive information or negative information. This kind of information cannot either automatically advance social prosperity, nor necessarily impair social interests. This kind of information can be either used or misused, or simply exists in itself. For example, collections of e-mail addresses can be used in sending advertisements of opt-out electronic marketing, or fabricating an advance-fee scheme. However, these addresses are value-neutral, as the user names and passwords are, too. This category of information is value-neutral from the standpoint that its content cannot be judged to be positive or negative as such.

The third category of information is valueless information. Some information has no value, for example, unsolicited commercial e-mail (UCE) or unsolicited bulk e-mail (UBE) without information of either a positive or negative value. The distinction between value-neutral information and valueless information lies in whether the value-neutral information does not induce a question of value judgment, and people cannot evaluate it as favourable or unfavourable; while valueless information induces value judgment, and people can evaluate it as neither favourably, nor unfavourably, but ordinarily as futile. In contrast to value-neutral information, valueless information can be used neither to promote social welfare, nor to degrade the social interests. This category of information is valueless by virtue of the fact that its content is valueless. However, the process may impair the normal order of the cyberspace by disseminating and transferring such information through information systems with malicious intent. The transmission of the valueless information exploits the bandwidth,[8] forming a worthless data flux and wasting the receiver’s time to deal with it. If the fact is of high ambiguity, the users have to spend time to browse around the information; even if the matter is of high certainty, the users also have to spend time removing the information. Even though each user wastes merely a few seconds or minutes, the time wasted by millions or even billions of users will be a substantive quantity. The process will virtually diminish the efficiency and increase the expenditure.

The fourth category of information, information with negative value indicates that the appearance, existence, and dissemination of information are detrimental to the stability of the state, public order, and individuals. It does not exist without the intervention of human factors. Some are created with malicious intent, for instance, a computer virus;[9] some are created from a contradiction within one’s value concept, in which he or she regards it as legal and beneficial to deal with such information as adolescent pornography, hate speech, etc.; some information is falsified information, fabricated with the purpose for defrauding and obtaining property or other benefits, or for disparaging, defaming, blaspheming, etc. To reproduce, sell, promulgate, publicize such information are all measures that cause monetary losses or other damage to others.

The introduction of negative information into information systems poses a series of risks that may lead to perilous and erroneous decisions, and cause impairment, suicide, and calamity. The risk of these threats necessitates an increasingly higher level of cybersecurity guaranteed by diverse specific services, with increased expenses and personnel. The entire society, from individuals, organizations to governments have to deal with the misinformation, manipulation of public opinion, and onslaughts against the social order and interests.

It is necessary to note that information with negative value can be converted into information with positive value once that information is recorded and stored by judicial agencies as evidence to hold the fabricators and disseminators liable. This does not indicate that the value of information changes, rather, that the information is used to prove the existence of the actus reus by its specific negative value. It is necessary for success in the prosecution of crimes related to information with negative value to seize information as evidence. The application of evidence rules should not pose any obstacles for the admissibility of information as evidence.[10] It should be granted because of its evidential weight.[11] Therefore, information should be differentiated in both substantive criminal law and criminal procedural law.

Besides the above four categories, there is a fifth category of information the value of which is disputable in the legal sense. That is to say, the criteria for evaluating the information are different in different countries. For instance, in some countries adult pornography is protected as free speech by the constitution and other laws, while in other countries its creation, production, duplication, publication, transaction, and dissemination are strictly forbidden. Furthermore, information can constitute a kind of political propaganda, which is also granted a different legal position in different countries, some having a high degree of free speech, and others having tight laws of political libel, and so forth.

Although information can be distinguished according to subjective judgment, it does not in itself represent virtue or vice. The pervasiveness of information does not constantly push forward social development and facilitate the maintenance of the legal order. Through technological supremacy, all kinds of information play certain roles, exert their influence, and gain markets. They are all regulated, intercepted, and monitored. Similarly, they all bear the risk of unauthorized access and destruction. In addition, it is possible to obstruct positive information by legislation and court rulings, while negative information may be protected erroneously. Accordingly, information products and services, sources and destinations, storage and flux, domestic and international information, and public and credential information bring about the complicated process of value judgment. In this article, except when otherwise mentioned, the term “information” is used in a positive sense.

The full power of information has been realized through ICT, which has a broad impact on social lives, including maintaining the common traditions through improving the accessibility of information about religious practices; keeping cultural continuity through access to more information; enabling governments, commercial businesses, news and media organizations, as well as educational organizations to perform their functions well; and increasing collective activities and interests through an improved work process and social interaction (Cnaan and Parsloe 1989; Committee to Study the Impact of Info, National Research Council Commission of the U.S. 1994).

Simultaneously, due to the accelerated accumulation of information, the management of information poses a great challenge to the public and private sectors (Daler 1989, p. 13). Both internal and external threats may cause unexpected loss to individuals or organizations. The resources invested on information management have to be increased. In turn, information systems will further propel the advancement of the society.

Information and the legal gap

Digital information is a novel product of technological progress aimed at promoting social welfare through improving productivity. Information and other products of information technology, however, do not always play a positive role as people sometimes expect. In fact, many human expectations are left vacant in social reality. Society never previously got rid of unforeseeable trouble for information of a positive value and that of a negative value was not easily distinguishable or filterable before information systems came into being. Nowadays, both the information itself and the relevant technology have a significance within the legal framework, because they should be either protected or prevented by law. Legal activities can involve information and ICT in different ways. The conventional legal notion is to be innovated to accommodate the inevitable role of information. The existing legal coverage should be extended to facilitate the protection or prevention of information processing and information abuse. Furthermore, co-operative preparedness and jurisdictional adequacy are required for promoting the effectiveness of law enforcement.

Information and communications technology takes the traditional society into a brand new stage that people call the information age. The existence and development of the information society requires a feasible social environment. The primary tasks that the legal framework bears are to provide legal assurance for the healthy and orderly development of information and telecommunications, and electronic and mobile commerce. Law does so through facilitating growth and eliminating obstacles. The information society is accompanied by various concerns about data security and privacy protection. The prevalence of insecurity and infringement threatens the whole environment of the new technology, new economics and new welfare. Such insecurity and infringement lead to the creation of defensive and remedial legal instruments against cybercrime, composed of both substantive and procedural provisions, and of both domestic and international legal adequacy. The complete legal structure of the information society can be illustrated as the following.

Table 2. Facilitative Law, Protective Law and Remedial Law

Categories	Facilitative Law	Protective Law	Remedial Law
Functions	Facilitating growth, eliminating obstacles	Avoiding insecurity, preventing infringement	Domestic criminalization, and international harmonization
Coordinated sectors	International forum, Domestic forum	Public sector, private sector	Public sector, private sector

The topic of this article contains no more space for facilitative law. The following sections are devoted to analysing the legal gaps accompanied by the proliferation of information systems.

The lag of a legal notion

Many scholars regard information as the third form of protective object in criminal law, alongside person and property. Accordingly, the criminal-law theory has been adjusted to contain the new protective object. Some others, however, insist that information is not the third protective object in criminal law; rather, they consider it as belonging to the category of property.[12]

They have criticized both the claim that information is the third protective object and the claim that information is not a protective object covered by criminal law. Conventionally, “information” in the form of digits was not previously covered and thus not protected explicitly by criminal law. Just as traditional economic doctrines maintained that only land and manufacturing rather than the service sector produced real wealth (Stonier 1983, p. 25), traditional legal theories maintained that only wealth represented or produced by land and manufacturing deserved legal protection. However, once the requirement to protect information emerges, conventional concept has to meet the needs of social development. Therefore, to say that information was not and should not be protected by criminal law is outdated. In fact, the majority of scholars and legislatures have not accepted that it should be protected.

Information has been protected by criminal law in two ways. While there are people suggesting that law should not protect information, some others assert that information can be protected by a means equivalent to the protection of property. That is to say, information should be categorized as being in the same domain as property. People consider expanding the arm of criminal law to information just as they did to electricity.

On the other hand, from ancient to modern times, criminal law has in effect been handling crimes related to information in different forms other than the electronic one, such as libel, perjury, forgery, blasphemy, hate speech, copyright, trademark, patent, and so forth. In practice, information does broadly cover those specific traditional forms, such as oral, written, and printed forms, and more recently the forms stored, and transmitted by electronic, magnetic, and optical carriers, including the telephone, facsimile, radio, television, satellite, and nowadays computers and networks. When people face digitally computerized information, they pay a lot of attention to the existence of information in traditional forms, and thus give new life to traditional information crimes. Our general notion should be changed in order to adjust to the new ways of “thinking, writing, arguing, and valuing” in the information society (Lanham 1993, p. 229). The semantic practices of the latter society are to label everything with a mark of “information” or to refer to its physical vessel “the computer” or to “the network.”

It is an issue of “concept innovation” rather than criminal-law reform to recognize this point, but this concept innovation is necessary during criminal-law reform. Many crimes can be reconsidered in the light of the prevalence of the concept of information. With electronization, computerization, digitalization, automatization, and networking, these crimes become more apparently characterized as involving information. This justifies a wide expansion of punishment for the traditional offences involving information or information systems. Anyway, criminal law cannot demand a further expansion except through our understanding of the nature of these crimes. The social and technological developments have been impacting on criminal law.

The legislative gap

Information is an emerging object protected by laws designed to maintain social order and protecting social benefits. The conventional penal code has been designed to address crimes involving “tangible and visible objects” (UNCJIN 1999, Paragraph 84). The increasingly higher value of information poses unprecedented legal challenges, demanding new legal responses (ibid). Information has a value for specific owners and users. Cybercrimes often involve the illegal obtaining or destruction of information. Because information, programmes, databases, computer services or computer time, are intangible and invisible, conventionally the law has not recognized what to do regarding them and has difficulty in providing even the definitions essential to defend this type of property involved (BloomBecker 1983, p. 11). Because of the lack of a clear definition of information as a valuable interest, the existing law does not easily conduce to successful prosecution. What is needed is that the existing laws should be adjusted to guard the abstract “information” itself rather than merely the computers in which the information is generated, the media in which the information resides, the cables by which the information is transmitted, or the Central Processing Units (CPUs) where the information is processed.

The sphere to be covered by the new laws includes the use of ICT to make existing crimes more perceptible, to enable the inclusion of new forms of existing crimes, and crimes that specifically attack information systems (European Information Society Group, EURIM 2002). Some countries have taken action to protect information as property in the traditional sense. On the other hand, some other countries exclude the concept of information from traditional crimes. Consequently, a noteworthy doctrine in criminal law rejects the independent position of information as one of the protective objects, which were conventionally confined to human being and property.

On the issue of information as property, there have been endeavours to adopt burglary law to acts of illegal access in which the cyberspace is supposed to be the equivalent of a domicile in genuine physical space.[13] Nevertheless, in this endeavour, people ignore the distinction between the threats of the two offences. What is endangered in burglary is not what is endangered in illegal access. In burglary, what is directly endangered is the security of life and property. In illegal access, what directly endangered is the security of information. Information is not the equivalent of life and property, though it is likely to be indirectly pertinent to life, and can generate benefits or cause losses, or measured by a definite amount of money. The offences of illegal access, nonetheless, belong to the activities infringing the security of information, but not the right or security of life or property.

By using the terms traditionally used to indicate the misconduct in traditional offences, the offences against information seem to bear a similarity to traditional offences. Yet many people still doubt how a pair of hands can hold a piece of digital information. Strangely, we can frequently take notice of a question as “Can information practically be stolen?” The genuine uncertainty behind this question is “does information really exist in material form?” In addition, the intrinsic meaning potentially ignores the entity of digital information before human organs can perceive it. They accept only information printed on paper, shown on a screen, spoken in a backroom, transferred into a smell, or into an impression in any other form. Nevertheless, it is significant to note that the fact of obtaining information includes a pure perception of the content of the material. It is not necessary for the information to be physically moved or copied. For instance, the U. S. law criminalizes access to a computer without sufficient authority and thereby getting financial information, or to any information controlled by the government, and access to any confidential information where interstate or overseas business is involved in the criminal act.[14]

In many countries, the law further details the act of “obtaining data” by different terms, such as copy, output, and theft. Digital information is not comparable to traditional property, and thus specific legal provision is required to protect it. However, it is undeniable that information is often related to property, or even health and life. The protection of information will surely facilitate the protection of property, health and life. In different countries, punishments for offences against property and person involving information have different starting-points. Some countries directly apply traditional law to these offences, such as the Penal Law of China.[15]

The Articles 285 and 286 create several new offences in respect of information or information systems. And another article, Article 287, provides for the application of separate provisions in the Penal Law to penalize traditional offences, such as financial fraud, theft, embezzlement, misappropriation of public funds and theft of state secrets, and would now cover computer information systems, other than in respect of illegal intrusion and destruction. The Article indicates that all the offences that can possibly involve computer information systems are to be punished. Some other countries merely apply the law to acts involving information, as the law in the U. S.[16]

The 18 U.S.C. § 1030 creates several new offences targeted at information and information systems, and expands several traditional offences to acts involving information and information systems. However, the default doctrine is that the offences which possibly involve information and information systems, but are not criminalized explicitly by law, would not be punished.

Nevertheless, criminal law is also confronted with some other gaps brought by the rise of computerized information, specifically, the sphere of illegal access to and illegal interference with information and information systems. The Internet has a universal impact on the ways by which people acquire and transfer information. The opportunities for cybercrime are correspondingly increasing with the extensive access to computers and the Internet. To protect against cybercrime, effective actions at the local, national, and global levels can be taken (Sofaer and co-workers 2001). Nevertheless, the overall contemporary legislative situation is unsatisfactory: not all jurisdictions are covered by laws criminalizing cybercrimes; not all legislatures are synchronous with the development of technology and the abuse of it (Gelbstein and Kamal 2002, p. 3); and nor can people update their conventional notions all the time.

The jurisdictional gap

The challenge to the contemporary legal system of digitalized information and its pertinent technology requires that countries with no law regulating the new object should enact laws, and that countries with such law should harmonize their laws. The starting-point of this harmonization and cooperation is the creation of coordinated definitions of information and information systems. Some countries provide definitions of information and information systems in their criminal laws, but there exist substantial differences, though in the primary aspects they are similar. In addition, the gap between the existing laws of different jurisdictions produces a safe haven[17] for the perpetrators of many kinds of offences involving information and information systems.

Conclusion

Being informed is not necessarily beneficial. Informed by useful information, people can better compete in the social life. Informed by useless information, nothing better or worse will happen than a waste of time. Informed by harmful information, people would possibly weaken their own competitive force. Presently, all kinds of information are transmitted through the same information systems. Interference with transmission of useful information causes people to be less informed. Interference with transmission of harmful information –and even useless information-also causes waste in identifying the value of information. Cybercrime can lead to both of these situations. With the introduction of information and information systems into society, protection and prevention become the imperative tasks that jurisprudence, legislation, and law enforcement are confronted with. There has not been adequate preparedness to respond to cybercrime. The process of recognition and acceptance requires much time. The imperative requirement is for people to be well informed about the loopholes the legal system has and how they can be altered.

Endnotes

1. It has long been recognized that both nature and society are changing. What Heracleitus said “One cannot step twice into the same river,” (Heracleitus 1979, p. 168) can be understood broadly as recognition of a changing world. The present day idea of change is accepted as the inherited nature of existence.

2. See Johnson (1970) stating that “Data system is used here to designate the artefact that consists of a digital computer, a control program, and an accessible library of programs and data.” (p. viii).

3. Uniform Computer Information Transactions Act (UCITA), Section 102 (35).

4. ibid, Section 102 (10).

5. See UN Recommendation on the Legal Value of Computer Records, adopted by the Commission at 18th session 1985.

6. Article 5, Model Law on Electronic Commerce of the United Nations Commission on International Trade Law, Annex of General Assembly Resolution A/RES/51/162.

7. United States v. Christopher Lee Adjani; Jana Reinhold, No. 05-50092 D. C. No. CR-04-00199-TJH-01 OPINION, 13 January 2006.

8. The bandwidth of a transmission channel is “a measure of the information-carrying capacity of the channel.” Daintith (2004), p. 38.

9. A computer “virus is a programme that is attached to or inserted into another programme...The virus may or may not do other things.” (Sadowsky and co-workers 2003, p. 47). In practice, viruses usually cause damages to the computer system.

10. Article 9.1, Model Law on Electronic Commerce of the United Nations Commission on International Trade Law, Annex of General Assembly Resolution A/RES/51/162.

11. ibid., Article 9.2.

12. Many of such arguments and discussion can be found in articles published in the 1980s, for example, BloomBecker (1981), pp. 16-17.

13. For example, entering the computer facility with the intent, by whatever means, of discovering another’s account number for purposes of stealing computer time constitutes burglary under California law and will be prosecuted. See Bruin OnLine (BOL), Information for New Users, 2004. Retrieved April 25, 2016, from https://www.bol.ucla.edu/cgi-ssl/accounts/newuser

14. 18 U.S.C. § 1030 (a) (2).

15. See Articles 285-287 of Penal Law of China, 1997.

16. See 18 U.S.C. § 1030.

17. The term “haven” is widely used by scholars or mass media to denote a country where there is no effective legislation or law enforcement for combating cybercrime, on academic materials, for example, McConnell International (2000), etc. News report, for example, William J. Kole, Romania becoming a haven for cybercrime, 17 October 2003, Associated Press. Retrieved 25 April 2016, from http://www.chron.com/disp/story.mpl/tech/2163754.html; The Nigerian Village Square, Nigeria: Haven for Terrorist Internet Communication? 4 August 2004. Retrieved April 25, 2016, from http://www.nigeriavillagesquare1.com/Articles/ oyesanya/ 2004/08/nigeria-haven-for-terrorist-internet.html. The terminology “haven for cybercriminals” is rather offensive to those countries referred to or implied.

References

Babbie, E. R. (1995). *The Practice of Social Research*. Belmont: Wadsworth Pub. Co.

Bjørn-Anderson, N. & co-workers. (1982). *Information Society for Richer and Poorer*. Elsevier Science.

BloomBecker, J. (1983). Conscience in Computer: A Law Day Perspective on Computer Crime. *Computers and Society*, volume 13, number 3, pp. 9-13.

BloomBecker, J. (1981). Employee Computer Abuse –What to Do? *The Los Angeles Daily Journal*, pp. 16-17.

Cnaan, R. A. & Parsloe, P. (1989). *Impact of Information Technology on Social Work Practice*. Binghamton, New York: The Haworth Press.

Coleman, J. S. (1990). *Foundations of Social Theory*. Cambridge, Massachusetts, and London, England: The Belknap Press of Harvard University Press.

Committee to Study the Impact of Info, National Research Council Commission (1994). *Information Technology in the Service Society*. Washington, D. C.: National Academy Press.

Daintith, J. (eds.). (2004). *Oxford Dictionary of Computing*, fifth edition. Oxford: Oxford University Press.

Daler, T., Gulbrandsen, R., Melgrd, B. & Sjølstad, T. (1989). *Security of Information and Data*. Chichester: Ellis Horwood.

European Information Society Group (EURIM). (2002). *Briefing No 34: E-crime – A New Opportunity for Partnership*.

Fisher, R. P. (1984). *Information System Security*. Prentice-Hall.

Gelbstein, E. & Kamal, A. (2002). *Information Insecurity: A Survival Guide to the Uncharted Territories of Cyber-threats and Cyber-security*. The United Nations Information and Communications Technology Task Force and the United Nations Institute for Training and Research.

Heracleitus. (1979). *The Art and Thought of Heracleitus: An Edition of the Fragments with Translation and Commentary*. Cambridge: Cambridge University Press.

Johnson, L. R. (1970). *System Structure in Data, Programs, and Computer*. Prentice-Hall, 1970.

Konig, E. C. & Davidson, C. H. (1967). *Computers: Introduction to Computer and Applied Computing Concepts*. Wiley.

Lanham, R. A. (1993). *The Electronic Word: Democracy, Technology, and the Arts*. Chicago: University of Chicago Press.

Molitor, G. T. T. (1982). The Information Society: The Path to Post-Industrial Growth, in Cornish, E. (ed.), *Communications Tomorrow - The Coming of the Information Society*. World Future Society, pp. 43-49.

Porter, A; Read, W. H. (1998). *The Information Revolution: Current and Future Consequences*. Ablex Publishing Corporation.

Rabin, J. & Jackowski, E. (1988). *Handbook of Information Resource Management.* New York, New York: Marcel Dekker.

Sadowsky, G., Dempsey, J. X., Greenberg, A., Mack, B.J., & Schwartz, A. (2003). *Information Technology Security Handbook.* Washington, DC: The International Bank for Reconstruction and Development.

Sofaer, A. D. & Seymour E. G. (eds.). (2001). *The Transnational Dimension of Cyber Crime and Terrorism.* Hoover Institution, pp. 35-68.

Sterling, B. (1994). *The Hacker Crackdown: Law and Disorder on the Electronic Frontier*, Austin, Texas: Electronic Release. Retrieved April 25, 2016, from http://www.gutenberg.org/dirs/etext94/hack12.txt

Stonier, T. (1983). *The Wealth of Information: A Profile of the Post-industrial Economy.* London: Methuen London.

Tapscott, D., Ticoll, D. & Lowy, A. (2000). *Digital capital: Harnessing the Power of Business Webs.* Boston, Massachusetts: Harvard Business School Press.

UNCJIN. (1999). International Review of Criminal Policy -United Nations Manual on the Prevention and Control of Computer-Related Crime. *International Review of Criminal Policy*, nos. 43 & 44.

Bibliographic information of this paper for citing:

Li, Xingan (2016). "Roles of information systems in socio-legal context." *Webology*, 13(1), Article 143. Available at: http://www.webology.org/2016/v13n1/a143.pdf