ISSN 2959-6149

Research on the issue of subrogation right in cyber security insurance

Ruoshui Zhang

Abstract:

As an important part of enterprise network security risk management, network security insurance provides loss compensation and risk underwriting for enterprises after the occurrence of network security events. At present, the cybersecurity insurance market continues to develop, and the insurance is aimed at the safety of property in the virtual network, in which when the enterprise is affected by the tort of a third party, resulting in damage to the virtual property, the effective exercise of subrogation rights greatly affects whether the insurance organization is willing to undertake to bear the risk, whether the insured is able to get the claim, and the application of the law. The place of occurrence of legal facts in cyberspace does not exist in the sense of the current law, therefore, the choice of jurisdiction is to apply the law of the location of the network operator, and to request the network service operator to assist in searching for the infringing web server Depending on the actual location of the third party in relation to the jurisdiction of the court, the right of subrogation is to be exercised by relying on the assistance of the local government.

Keywords: cyber security insurance, subrogation right, territorial jurisdiction, place of cyber infringement behavior

1.Introduction

1.1 . Broad Prospects for Cybersecurity Insurance

With the ever-advancing Internet, enterprises are increasingly dependent on digital technology, resulting in a surge in cybersecurity threats. A growing number of enterprises are now grappling with cyberattacks, data breaches, and various other security incidents, prompting them to recognize the criticality of cybersecurity risks and committing more resources to safeguard their digital assets and customer data. In this backdrop, traditional security measures may fall short in fully mitigating these threats. Consequently, the adoption of cybersecurity insurance as a potent risk management tool is gaining wider acceptance and recognition as an inevitable choice for enterprises.

Cybersecurity insurance, a vital aspect of enterprise cybersecurity risk management, offers enterprises loss compensation and risk underwriting in the aftermath of a cybersecurity incident. Indeed, it provides enterprises with a comprehensive risk management solution. By procuring cybersecurity insurance, businesses can secure timely financial assistance in the event of a cyberattack, data breach, or any other security incident. As cyber threats continue to morph, insurance companies are innovating and introducing insurance products tailored to enterprises' needs, including cyber liability insurance and cyber interruption insurance. Moreover, as enterprises' focus on cybersecurity intensifies, the development of cybersecurity insurance holds a promising future, with the market poised for further expansion.

1.2 . Network security insurance mechanism needs to be sound

In traditional insurance, once a tort occurs and the victim receives compensation from the insurance company, the insurer assumes the victim's position to exercise the subrogation right against the tortfeasor, aiming to recover the amount paid as compensation. Understanding the rationale behind why cyber insurance law should incorporate the insurer's subrogation right is fundamental to our comprehension and establishment of this system.

Some scholars argue that the subrogation system aims to prevent unjust enrichment of the insured. Specifically, when an insurance incident arises due to a third party's actions, resulting in damage to the insured property, the insured may simultaneously claim compensation from both the third party and the insurer. This could potentially lead to double compensation, contrary to the principle of 'prohibit unjust enrichment'. To prevent such enrichment, the insurer's subrogation system requires the insured to transfer their right to claim to the insurer.

Currently, this is a general consensus in insurance legislation. However, another viewpoint holds that exercising the insurer's subrogation right substantially reduces the total insurance payments, leading to a decrease in insurance premiums. This reduction, in turn, lightens the burden on

the vast majority of policyholders in society. This theory, from the perspective of insurance business operations, justifies the existence and importance of the insurer's subrogation right, further emphasizing its significance in promoting sound network security insurance.Therefore, the agreement and mechanism for exercising the right of subrogation should be fully considered in cybersecurity insurance contracts, so as to promote cybersecurity insurance for the public.

2. Significance of the exercise of subrogation rights

2.1 . Positive impact on insurance organisations

In the context of cybersecurity insurance, subrogation rights help insurance organisations to better manage and spread risks. In the field of cyber security, the value of virtual property may be difficult to accurately assess due to its characteristics, while the risks are inevitable due to the various forms of cyber attacks. Under such circumstances, insurance companies need to take into account the uncertainty of the risk and the possibility of bearing compensation when considering whether to assume the risk of cybersecurity insurance. The existence of the right of subrogation makes it possible for the insurance company to share the loss by recovering from the infringer after assuming the liability for compensation, which reduces the pressure of compensation on the insurance company and improves its affordability for cybersecurity insurance.

2.2 . Protecting the interests of the insured company

The right of subrogation is conducive to the protection of the insured's rights and interests and ensures that it can receive timely compensation. After a cybersecurity incident, the insured often needs to resume business and reduce losses as soon as possible, while the claims process of the insurance company may take some time. Without the right of subrogation, the insured may need to recover damages from the infringer on its own, which is time-consuming and inefficient. The effective exercise of the right of subrogation can ensure that the insured can obtain compensation in a timely manner, which reduces the economic losses suffered by the insured due to the cybersecurity incident.

In addition, the subrogation right is recognised as a claim transfer system based on the principle of insurance interest to prevent the insured from obtaining double benefits, which also has positive significance for the application of law and judicial efficiency. In cybersecurity insurance cases involving virtual networks, the legal application and cross-border recovery issues involved may be more complex. Through the right of subrogation, the insurance company, as the beneficiary, can directly claim its rights against the infringer, reducing the complexity and judicial costs for the parties involved, and facilitating the rapid resolution and fair trial of the case.

3. Determination of the place of online infringement

3.1 . Differ from the traditional infringement of the law application

3.1.1 . Network infringer actual location is difficult to determine

Unlike China's Civil Procedure Law, Article 23 provides: 'the litigation arising from contract disputes, by the defendant's domicile or the people's court of the place of performance of the contract jurisdiction.' And the supreme people's court on the application of the civil procedure law of the People's Republic of China on the interpretation of article 20 provides: 'the information network way to conclude a contract of sale, through the information network delivery of the subject matter of the buyer's domicile as the place of performance of the contract; through other means of delivery of the subject matter of the receipt of the contract for the place of performance. The contract has agreed on the place of performance, from its agreement. Purchase of goods on the Internet, and the shop to form a contract of sale, the shop by express delivery of goods to their residence. Now there is a dispute over the contract of sale, you do not have to sue to the court where the shopkeeper is located, but you can sue to the court of your own place of residence.' , the flow of data in the network becomes untraceable, as well as the definition of legal jurisdiction becomes complex and ambiguous.

There are many views in the academic community that the defendant's domicile is no longer appropriate as a jurisdictional connection point, because most of the tortfeasors do not use the real name and address on the network, the defendant's domicile can not be determined.

3.1.2 . Virtual location intervention judgement of the place of occurrence of facts

Looking around the world, the 'place of infringement' is defined as 'place of infringement' of the typical legislation such as Austria on 25 June 1978, 'Federal Law on Private International Law,' Article 48, paragraph 2, there are similar legislation in Armenia, Azerbaijan, etc.; the 'place of infringement' will be defined as 'the place of infringement', Azerbaijan, etc.; typical legislation defining the 'place of infringement' as the 'place where the result of the infringement occurred' is article 1219, paragraph

1, sentence 2, of the Civil Code of the Russian Federation, which entered into force on 1 March 2002, and the Netherlands, etc.; some States avoid the 'place where the infringement was committed'; the Republic of Slovenia, etc.; some States avoid the 'place where the infringement was committed', Some countries avoid defining the 'place of infringement' and use the 'fact giving rise to liability' as a connecting factor, i.e. the 'place where the infringement was committed' and the 'place where the result of the infringement occurred'; the 'place where the infringement was committed' and the 'place where the result of the infringement occurred' are also typical. That is to say, 'the place where the tortious act is committed' and 'the place where the result of the tortious act occurs' can be regarded as 'the place of the tortious act'. Typical legislation includes article 20, paragraph 1, of the Algerian Civil Code as amended in 2005, and there are also countries with similar legislation, such as Cuba and Jordan.

However, it is often difficult to determine the place where the legal fact occurred in the network, and due to the existence of virtual identity and anonymity, the actors can modify the IP address, use proxy servers and other means to hide their real identity and location. The transmission paths of information and data are often complex and varied, and may involve network nodes in multiple countries and regions. At the same time, encryption and privacy protection measures that may exist during data transmission make the flow of data in the network even more untraceable, further increasing the difficulty of determining the place where the legal facts occurred.

3.2 . Choice of territorial jurisdiction

The Supreme People's Court has attempted to avoid abusive choice of venue by limiting the order of choice of courts by plaintiffs in several judicial interpretations. Article 1 of the Interpretation on Several Issues Concerning the Application of Law to the Trial of Cases Involving Copyright Disputes over Computer Networks is more detailed: 'Cases of disputes over copyright infringement on the Internet shall be under the jurisdiction of the people's court of the place where the infringement was committed or the place where the defendant resides. The place of infringement includes the place where the network servers, computer terminals and other equipment are located to commit the alleged infringement. If it is difficult to determine the place of infringement and the defendant's domicile, the place where the plaintiff discovers the infringing content of the computer terminals and other equipment can be regarded as the place of infringement.' In cybersecurity insurance, there is no place of legal fact in cyberspace in the sense of the current law, so the law of the location of the network operator applies to the choice of the place of jurisdiction of the third-party infringement when it occurs. In order to effectively protect the rights and interests of the insured and ensure the implementation of the insurance contract when the infringement of the third party occurs, the law of the location of the network operator may be the optimal solution.

As a key player in cyberspace, the network operator usually has clear legal jurisdiction in its location. In the case of cybersecurity insurance, the network operator bears the responsibility of maintaining network security and safeguarding user information, and the legal system of its location often has relevant provisions and constraints on infringement behaviour in cyberspace. Therefore, taking the law of the location of the network operator as the applicable law is conducive to the effective regulation and punishment of network infringement and the protection of the legitimate rights and interests of the insured.

In addition, choosing the law of the location of the network operator as the applicable law also helps the smooth implementation of the insurance contract and claims, which can reduce disputes over the application of the law and improve the operability and efficiency of the implementation of the insurance contract.

4. Coverage for the insured's acts of disposition of third-party rights

4.1 . Assistance from the government of the actual location of the third party

Due to the virtual and cross-border nature of cyberspace, the identity and physical location of the infringing third party is difficult to be obtained directly, so in this case, it is necessary to rely on the assistance of the government of the actual location of the third party, through judicial investigation and assistance, to obtain the identity and address information of the infringing third party, in order to provide the necessary support for the exercise of the right of subrogation. Secondly, once the identity and actual location information of the infringing third party has been determined, the insured can rely on the local government's judicial institutions and legal procedures to recover and dispose of the infringing third party.

4.2 . Security obligations of network service providers

The duty of security can be traced back to von Bar's European Comparative Tort Law's introduction to the German law duty of security of interactions. In the book, von Bar categorised the duty of security as a general duty of care at the level of tort of omission, and put forward the so-called general duty of security of interaction (allgemeine Verkehrspflichten). Chinese scholars put forward the con-

cept of 'general safety duty of care', and understand it as the subject engaged in certain social activities, such as the activity has the risk of harm to others, the obligation to prevent others from suffering damage within reasonable limits. This is tantamount to stipulating that general civil subjects have a duty of care to guard against unspecified dangers, a requirement that is obviously too harsh.

However, unlike direct torts, most torts under cyber security insurance are indirect torts, with the added role of direct tortfeasor between the security obligor and the victim. Although the Civil Code does not explicitly impose a security obligation on ISPs, it has long been and is heavily applied in judicial practice. Legislatively, Article 38(2) of the Electronic Commerce Law (hereinafter referred to as the E-commerce Law) clearly stipulates that an e-commerce platform that fails to fulfil its duty to examine the qualifications of the operators on the platform or fails to fulfil its security obligation to the consumers, which results in the consumer's damage, shall bear the tort liability. Therefore, the network service provider that has not fulfilled its security obligation should also provide necessary assistance to the insurance company in exercising its subrogation right.

References

Yu, Lili (2008) 'Reconstruction of the Basic Theory of Subrogation Claims of Insurers', Law Review, No. 4, 2008.

WANG Ni Jie (2020) 'On the Boundary of Security Obligations of Network Service Providers and Its Construction - Taking the Interpretation of Network Tort Rules in the Civil Code as a Perspective', Rule of Law Research, No.1, 2022.

Yu, Haifeng (2010) 'A General Study on the Territorial Jurisdiction of Civil Litigation in Network-Related Cases - Based on the Spatial Positioning of the Place of Legal Facts', Legal Science, No. 5, 2010.

Chen, Weizuo (2012) Comparative Private International Law: A Comparative Study of the Legislation, Rules and Principles of the Law Applicable to Foreign Civil Relations, Law Press, Beijing, 404; Zou, Guoyong (2011) 'Comparative Private International Law: A Comparative Study of the Legislation, Rules and Principles of the Law Applicable to Foreign Civil Relations'.

Zou, Guoyong (2011) Selected Legislation on Foreign Private International Law, China University of Political Science and Law Press, Beijing, 109; Symeon C. Symeon.

Symeon C. Symeonides. (2014) Codifying Choice of Law Around the World: An International Comparative Analysis [M]. New York: Oxford University Press, 59.

Sun Jilu (2003) Research on Insurance Subrogation Rights, Legal Science, 2003, No. 3.

Qin Youtu and Fan Qirong (2013) Insurance Law, Higher Education Press 2003, p. 241.

von Bar, Verkehrspflichten.(1980) Richterliche Gefahrsteuerungsgebote im deutschen Deliktsrecht, S. 313.

Wen, Shiyang and Liao, Huanguo (2003) The General Duty of Care for Safety in Tort Law, Wang, Liming, eds: The Civil Code - A Study of the Law of Tort Liability, People's Court Publishing House, 2003 edition, p. 91.

Chen Ji (2006) network infringement disputes of jurisdiction [J]. Journal of Jimei University (Philosophy and Society), (1):41.