Science & Technology Development Journal – Economics - Law and Management, 6(1):2175-2183

Open Access Full Text Article

Research article

Improving Vietnamese law on the pre-action collection of evidence of law violations in cyberspace

Dao Trong Khoi[1,2,*]

Use your smartphone to scan this QR code and download this article

ABSTRACT

In this technological era, illegal acts are surging in cyberspace and causing considerable damage by exploiting the fast and convenient features in connecting and making online transactions. Obtaining evidence and information related to those acts is a prerequisite for the victims of law violations in cyberspace to use legitimate tools to secure their rights and interests. Such an activity must be conducted as soon as possible, even before the proceeding starts to prevent the important evidence and information of the violators from being permanently dispersed or deleted. However, such data is often stored by an opposite party or placed under the management of third parties such as banks, internet service providers, and social media platforms. These parties tend to refuse information disclosure due to the conflict of interests, assurance of confidentiality, and other business issues. In this regard, Vietnamese civil procedure law still encounters several difficulties for the victims to collect evidence at the pre-action stage. The law has neither clarified the victims' right to request the evidence holders to disclose nor provided the victims with any other effective measures to support such collection in this crucial period. Meanwhile, the procedural law of foreign jurisdictions, e.g. the UK and the Netherlands, is integrated with effective mechanisms to deal with this specific issue. In general, such mechanisms entitle the victims to request the court to order the evidence holders to disclose crucial evidence of the violations and information about the violators before the commencement of a civil action. Using both doctrinal and comparative methods, this article examines these foreign schemes to determine several vital points for improving Vietnamese civil procedure law regarding the request for court assistance in collecting evidence at this pre-action stage.

Key words: procedure law, evidence collection, law violation, cyberspace, pre-action stage

[1]*Faculty of Business, FPT University Hanoi, Vietnam*

[2]*School of Law, Vietnam National University, Hanoi, Vietnam*

Correspondence

Dao Trong Khoi, Faculty of Business, FPT University Hanoi, Vietnam

School of Law, Vietnam National University, Hanoi, Vietnam

Email: khoidt3@fe.edu.vn

History

- Received: 23-5-2021
- Accepted: 29-9-2021
- Published: 25-12-2021

DOI : 10.32508/stdjelm.v6i1.832

VNU-HCM Press

AN INTRODUCTION TO THE OBSTACLES IN COLLECTING EVIDENCE OF ILLEGAL ACTS IN CYBERSPACE AT THE PRE-ACTION STAGE

Law violations in cyberspace are commonly reported and causing a huge amount of damage to individuals and organizations [1]. By exploiting the features of the Internet, including fast connection, easy transaction, and anonymity, common cyber violations such as online fraud, selling fake or low-quality goods, distributing malicious code, spreading fake news or superstitions, intimidation, stealing personal information can be conducted easier with a lower possibility of being punished. The victims of those violations could only invoke legal tools to protect their legitimate rights and interests if they promptly collect adequate evidence and information related to the violations. Without such evidence, the victims have no basis to either file a proper petition or persuade the court that their claims, protests, and requests are well-grounded and lawful.

A successful collection of evidence for such a purpose typically requires two conditions, namely (i) adequate and (ii) timely. Regarding the former, to adequately collect the important evidence and information, the victims must have access to all possible sources containing the data relevant to the violations and the alleged violators. Collecting evidence from the available sources under the victims' management (i.e., emails, chatboxes, transaction bills) is usually not complicated. However, accessing the sources which are 'unavailable' is more troublesome, as those are normally held by the opposite party or by third parties to the dispute. For instance, information about an account holder engaging in cyber fraud is normally kept by the bank. Evidence of spreading malicious code associated with the violator's IP address is stored by the hosting company (ISP). Details of a scammer via phone calls shall be under the management of a telecommunication service provider. Several third parties (i.e., witnesses, possible co-plaintiffs, official authorities) might be willingly or legally required to disclose the

Cite this article : Khoi D T. **Improving Vietnamese law on the pre-action collection of evidence of law violations in cyberspace** . *Sci. Tech. Dev. J. - Eco. Law Manag.;* 6(1):2175-2183.

evidence when being requested. However, most of them such as intermediaries involved in the transactions (platforms, social networks, workgroups) or related service providers (banks, retailers) tend to refuse that request due to the conflict of interests and other legal and business issues. For instance, their contracts or terms and conditions might include a confidentiality clause, deterring them from revealing their customers' information. They are also not bound by laws or have no contractual obligation to provide evidence, and such a reveal of their customers' and partners' secrets might decrease the companies' reliability and reputation.

For the second condition, time is precious in dealing with cyber violations because the evidence, information, and related assets can be dispersed easily and rapidly in cyberspace. That data might only be stored on clouds, servers, or backed up in hard storages of third parties, but they commonly have the policy to wipe to make room for new data after a short period. Thus, the victims shall collect evidence as soon as possible and should not wait until the commencement of the proceedings. Additionally, when the proceeding starts, a summons shall be served to the violator, allowing them to notice an incoming lawsuit and "wash their dirty hands" quickly. Besides, being unknown of specific details of the violations and violators, the victim may not even know who exactly committed the violations and therefore fail to form a legitimate petition.

RESEARCH METHODS

The points above indicate that victims of law violations in cyberspace need State support to promptly collect evidence from any evidence-holder even before the commencement of the case. Using two fundamental legal research methods: doctrinal and comparative, this article firstly analyzes the Vietnamese civil procedure law to find any prospective legal basis that victims might resort to requesting court assistance in collecting evidence at the pre-action stage. Afterwards, the research examines the procedural legislation and case laws of the United Kingdom and the Netherlands to determine their available schemes supporting the pre-action collection of evidence. These international experiences might be considered as valuable references for Vietnamese procedure law to develop our system to secure the legitimate interest of those victims to obtain evidence at this crucial stage.

RESULTS

Vietnamese laws on evidence collection in the initial period of settling the case

The 2015 Vietnamese Civil Procedure Code ('CPC') contains certain regulations providing the rights to collect evidence in and around the initial period of settling the case, which might assist the victim in collecting the evidence needed. For instance, Article 70.7 and Article 97.1 CPC allow the victim to request the court to issue a decision demanding evidence holders to disclose relevant documents and evidence when he/she is 'unable to collect himself/herself'. Article 106.2 CPC then prescribes the request's content, the corresponding deadline to disclose and consequences for disobeying that decision. Article 110 CPC also specifies that if the destruction of evidence is ongoing or highly possible, the victim can ask the court to protect the evidence by applying measures including sealing, seizing, photographing, recording, restoration, examination, making minutes and others. Additionally, Article 106.1 CPC entitles the victim to request an evidence-holder to disclose evidence directly, and the holder shall either reveal or explain legitimate reasons for non-compliance within 15 days.

However, wordings of Article 97.1(e), 70.7, and 106 CPC particularize that these rights can only be used by an 'involved party'. Article 68.1 CPC then describes an 'involved party' as a litigant, such as a plaintiff claiming that its legitimate rights and interests have been damaged. The Code does not clarify precisely when a victim becomes a plaintiff under the civil procedure, and it is logical to assume that this moment is when the court accepts the case[2]. However, among the list of exclusive rights and obligations given to an 'involved party' at Article 70 CPC, there is an obligation 'to advance court fees and charges, and pay court fees and charges and other expenses' – which must be fulfilled by a yet-to-be-plaintiff entity before the court proceeds to accept the case. Nevertheless, from the *de facto* application of the Code and the expressed wording of Article 70.7 and 97.1(e) CPC, the victims can only resort to this right when they become an 'involved party' after the courts accept the case. However, waiting until that moment might be too late, depriving them of obtaining most of the needed evidence.

Besides, in urgent situations when important evidence and assets might be rapidly dispersed or destroyed, Article 111 CPC entitles the victim to request a court's decision applying provisional measures listed in Article 114 CPC concurrently with the submission

of a petition[2]. Although the list indexes many measures such as seizing, freezing, prohibiting, and postponing, no measure explicitly demands the evidence holders to disclose. Only one measure mentioned in Article 114.12 and specified by Article 127 CPC might be helpful in this situation. Accordingly, the court may force a party to perform 'certain acts' if the non-performance or performance of such 'certain acts' by that party may 'affect' the resolution of the case. The definition of such 'certain acts' has not been clarified, and the court retains wide discretion in determining whether a particular act might 'affect' such a resolution. Article 8 of Resolution 02/2020/NQ-HDTP of the Justice Council of the People's Supreme Court explains that a resolution might be 'affected' when a party either commit a performance or non-performance which 'prevents the collection of documents and evidence' or 'conducts any other act' similarly deterring the resolution of the case. For instance, this measure could be applied to force a person, who obstructs the authorities' on-site inspection and appraisal, to open his door(s) to facilitate the inspection. Given that this clause is for overcoming obstacles to obtain evidence, one may argue that the clause might be invoked by a victim of cyber violations to request the court to force the evidence holders to perform 'certain acts', such as disclosing or allowing access to crucial evidence. However, such an ambitious interpretation has not been confirmed.

Additionally, other obstacles might negate the victim from applying for that measure. Regarding Article 111 and 189 CPC, concurrently with the measure application, an applicant shall submit a proper petition containing 'name(s), place(s) of residence, place(s) of work, phone number(s), fax, e-mail, etc. … of the defendant(s)'. Article 133 CPC further requires the victim to provide compelling evidence for justifying the necessity of such a measure. Thus, there is a causality dilemma in this situation, as the victim has no alternative but to seek a court's decision to request disclosure of the violators' details and evidence of the violations. However, a mere amount of evidence from available sources might be insufficient to convince the court to issue the decision, and they may not even know the names and details of future defendants. Since this right could only be used 'in the course of settling cases' concurrently with the proceedings' start, waiting until that moment might also be too late.

Given that the above provisions are inapplicable at the pre-action period, the victim could only resort to Article 97.1(d) CPC to directly request the evidence holders to provide a copy or needed materials related to the resolution of the case. However, the CPC fails to clarify the connotations of this right, its procedures for execution, any state support for such a request, or any consequence for non-compliance. Such a failure *de facto* inactivates this right and deprives the victim of any chance to obtain evidence from the third party at this stage.

International experience in supporting the pre-action collection of evidence

By contrast, several countries in both Common law and Civil law systems acknowledge the legitimate interest of the potential plaintiffs to collect evidence of the cyber violation even before the commencement of the case. For instance, the procedural laws of both the United Kingdom and the Netherlands provide such victims with the court's aid to request the evidence holders to disclose relevant evidence, which is described hereinafter.

the United Kingdom (UK)

English civil procedure law provides the victims with several ways to obtain evidence from unavailable sources at the pre-action stage as a part of the 'disclosure' procedure.

Regarding Article 31.16 of the UK's Civil Procedure Rules, the victims might strengthen their potential claims by applying to the court to disclose evidence held by the opposite parties before the proceeding starts. Following the judgment of Lord Briggs in *Hands v Morrison*[3], at first, the applicant shall surmount several hurdles, namely (i) the applicant and respondent are likely to be future parties to subsequent proceedings; and (ii) the disclosure shall be desirable in order to dispose fairly of the anticipated proceeds, assist the dispute to be resolved without proceedings, or save costs. Both of these hurdles require no specific standard; thus, a mere prospect in principle might be sufficient to overcome. Second, the court shall carefully examine the categories of documents sought to check the reasonableness for such discretion. Third, the application must be backed by evidence showing that at least a potential case might happen. One might observe that these tests are tight to meet, especially the requirement of 'fairness'[4]. The scope of the disclosure is also restricted to only specified documents held by the potential defendant(s).

For requesting a pre-action disclosure of the evidence kept by third parties, the victims shall resort to a *Norwich Pharmacal* order whose name and principles derive from *Norwich PharmacalCov Customs and Excise Commissioners* [1974] AC 1333. For the grant of this order, three conditions below shall be satisfied:

First, wrongdoing must have been carried out, or arguably carried out, by an ultimate wrongdoer[5]. This

'wrongdoing' might be any legal violation, including a crime, a tortious act including fraud, intentionally wrongful conduct and defamation, contempt of court, breach of the contract, breach of statutory duty, breach of confidence, and others[6]. The wrong must be identified by the applicant and backed by sufficiently cogent evidence to prove that such an activity occurred and a case against it is more than barely capable of serious argument[7].

Second, the third party must be 'mixed up in' so as to have facilitated the wrongdoing, which means that such a third party must connect with the wrongdoing to the extent that 'enable the purpose of the wrongdoing to be furthered'[8], innocently or incentively, with or without the knowledge of the wrongdoing[9]. The 'mere witness rule', which allows a witness to refuse to disclose by the reason that the witness's information can still be sought through oral testimony or a *subpoena duces tecum* in later procedures, is not applicable to this circumstance. This is because in the application of this rule, and the witnesses refuse to disclose at the pre-action discovery, the victims only have insufficient information of the wrongdoing and the wrongdoers and cannot even initiate the action to collect evidence at the oral testimony afterwards[9]. Thus, being a mere receiver of a document, an administrator of the online platform or service providers are sufficient for being obligated to assist the victims in finding evidence for their cases, given the nature of the wrongdoing and its purpose are serious enough[8]. In cases like *Golden Eyev Telefónica*[7] and *RFU v Viagogo*[10], internet service providers and operators of websites were subjected to this order because their customers and users exploited the system to commit unlawful acts. The applicant shall also prove that the involved party can provide the requested information.

Third, there must be the need for an order to enable action to be brought against the ultimate wrongdoer[5]. The court shall determine such necessity by searching for any other practicable means to seek evidence rather than this order. If such an alternative(s) exists, the applicant shall present its previous efforts to use that alternative(s) and explain why the alternative(s) is useless in reaching full disclosure. However, this order needs not to be the last resort[8]. For a further determination, the court can consider the proportionality of such an order by using ten other factors listed by Lord Kerr in *RFU v Viagogo,* including the strength of the possible cause of action expected by the applicant, whether this might deter the similar future wrongdoing, the degree of confidentiality of the information requested, privacy rights, and others.

Following the grant of such an order, the involved party is obligated to provide 'full and frank' information connecting to the violations and the wrongdoers. The scope of disclosure granted has been widened substantially, from disclosing the identity of persons who might be a prospect defendant in *British Steel v Granada*[11], to the disclosure of relevant evidence for tracing the fraudsters and lost assets in *Banker Trust*[12], and even to determine whether tortious conduct occurred in *P. v. T. Ltd.*[13]. This broad scope effectively supports the victims of cyber violations in strengthening their claims, as the 'full information' sought include both known and unknown evidence and information needed, such as details of an email sender [8], the IP address of a website's user[14], or the address of a man who the requester only knew his phone number[15].

Furthermore, the order could even be granted without notice to both the requested party and the wrongdoer to prevent the chance that the requested party may somehow inform the wrongdoer. In urgent cases, the court allows the applicant to submit skeleton arguments and evidence before the hearing and mostly focuses on the appropriateness of that order in the hearing[16]. According to *British Steelv Granada* , the applicant is not obligated to pursue litigation after obtaining evidence but can only use the data for future proceedings[11]. Finally, anyone disobeying or ignoring a court order might be found guilty of contempt of the court, which might result in a fine, asset sequestration or even twelve months of a custodial sentence[17].

the Netherlands

Although the Dutch law does not allow a full discovery similar to that of the UK, it does allow a litigant or potential litigant to obtain evidence from the opposite parties and any third party before proceeding. The Dutch Supreme Court (*Hoge Raad*) stated in its judgment ECLI:NL:HR:2015:1834 that, according to Article 843a of the Dutch Code of Civil Procedure ('DCCP'), any party showing a legitimate interest might request the court to order a third party or a future respondent to provide a copy, extract or allow the inspection of certain documents regarding a legal relationship to which it or its predecessor is a party[18]. Generally, three cumulative conditions must be surmounted for a grant of such an order[19]:

First, the applicant shall demonstrate a 'legitimate interest' in disclosing the requested documents. For instance, a purpose such as strengthening a claim in pending proceedings or preparing for future litigation might be sufficient to pass this test. However, the specific criteria for this have not been consistently explained, and the court retains its discretion

in finding such a 'legitimate interest' in factual details and evidence provided by the applicant[20]. Generally, bare speculation such as asking for disclosing documents which are suspected to be relevant or possibly strengthen the claims might be refused at ease[21].

Second, the applicant shall certainly specify all evidence and documents requested in its application and explain the relevance of those to the aforementioned 'legitimate interest' to prevent 'fishing expeditions'[22]. The applicant must not specify all small detail such as name or date of each document, but should clarify as specifically as possible the documents or at least their categories to maximize the chance of being granted. For example, characterizing 'all correspondence between two people named X and Y regarding the content A in the year of B on the platform C' might be sufficient[23]. The documents sought must also be at the disposal of or held by the requested party.

Third, the disclosure shall relate to a legal relationship to which the applicant is a party. This legal relationship could be any civil relationship such as a wrongful act, an alleged tort, or a contract[24,25]. The existence of such a shortcoming or wrongful act shall be sufficiently proven by reliable available evidence and facts[20].

However, the court shall consider whether any of the restrictions below may apply and deter it from granting the order:

- the document-holders have a duty of confidentiality regarding such documents by the virtue of his or her administrative position, profession or employment (e.g., lawyers, doctors, notaries). The court must consider whether the requester's interest in the disclosure may prevail over the holders' interest in complying with duties under their service provision contracts or prescribed by laws[26].
- the holders have compelling reasons or a serious interest to refuse to disclose. The court retains its discretion in weighing such rationales. For example, in *Claimants v. Food for the Mind*, the document-holder argued that the document sought, which is a purchase agreement, contains business-sensitive information and should not be disclosed. However, the court stated that such a mere assertion based on the confidentiality clause is not 'compelling' enough, and without any further evidence, the court cannot refuse to grant the order[27].
- the proper administration of justice can still be safeguarded without releasing such documents as if there is another alternative(s) to seek evidence, such as witness examination.

Although the scope of disclosure of this Article is not a 'full information' and only restricted to those documents sought, it might still be broad in other senses. For instance, the Amsterdam District Court (*Rechtbank*) issued an order to require the requested party to disclose all bank statements of an account for 13 years from 1992 to 2005[28]. The definition of 'documents' at this point also includes data on a data carrier; therefore, any cyber evidence and information might also be reached. In some circumstances, the court even determines the manner in which a copy, extraction or inspection of the documents can be sought.

It is not required that proceedings are or are expected to be brought following a grant of the order. The applicant can request this in either preliminary relief proceedings or ongoing proceedings on the merits[29]. The orders sometimes give a tight deadline such as 48 hours from its issuance, and a failure to comply may result in a penalty of, in some cases, up to € 5,000 per day, with a maximum of € 500,000[27,30].

DISCUSSIONS AND SUGGESTIONS

Experience in the above jurisdictions assures that the support of the court is essential for a possible plaintiff and especially a victim of cyber violations to collect evidence from the pre-action stage. Under the courts' aid, applicants in the Netherland succeed in requesting for all email correspondence between wrongdoers[31], or complete audit files of a company[32]. Other victims in the UK have exploited this to identify the wrongdoers unlawfully reselling tickets online[10], to request Google to disclose details and the IP address of libelers[33], to ask Facebook to provide evidence and details on misuse of personal information and defamation[34]. Without the court's supports, the victim cannot adequately and promptly collect evidence held by any third party who refuses to disclose, and therefore, might not even know the identity of the alleged violators.

The aforementioned analyses indicate that Vietnamese civil procedure law should be improved to uphold the legitimate interest of a victim of cyber violations to collect adequate evidence timely. The victim usually has to wait until the proceeding starts to exercise the rights and measures given by CPC, but as described above, that moment might be too late to obtain evidence in this ever-changing cyberspace. Thus, this improvement is crucial and inevitable. In the process of such development, attention should be paid to several important points drawn from relevant laws of foreign jurisdictions such as the UK and the Netherlands where advanced mechanisms have been developed to deal with such a topic.

First, to incorporate this mechanism into the Vietnamese CPC, an entirely new clause similar to the Dutch's concept at Article 843a DCCP should be added as an 'application' in the civil procedure. Given that such assistance may substantially affect the evidence holders' legitimate rights and interests, conditions and procedures to apply such a mechanism shall be specified in detail, rather than being formed as supplements or clarifications of existing articles on rights and measures in the CPC. The addition will introduce a new procedure before the commencement of the case. Accordingly, a party is entitled to request the court for the issuance of a decision demanding the evidence holders to disclose evidence and information related to wrongdoing in which such holders are involved. An amendment as such, therefore, shall be thoroughly considered by legislators rather than being clarified in a precedent or a resolution of the Supreme People's Court.

Another option is incorporating this into the provisional measure list at Article 114 CPC to exploit existing procedures formed in chapter VIII CPC to execute the new mechanism. However, the issues described above may continue as the victim must concurrently submit a petition specifying the yet-to-be-known details of the violators. Besides, strictly requiring the victim to be a future litigant might *de facto* inactivate this mechanism. Usually, the victims may resort to this assistance when being unconfident to straightly start the lawsuit with the limited evidence possessed straightly; thus, such a strict requirement may frighten those uncertain victims and discourage them from using it.

Second, regarding the conditions for granting such a decision, four hurdles below shall be all surmounted:

- the existence of wrongdoing in which the applicant who is a party shall be proven by all available evidence and information collected
- The requested party must relate to that wrongdoing by being 'mixed up in' or 'furthering' that wrongdoing as suggested by the British concept. Therefore, being a mere receiver of information or organizing a platform for unlawful transactions are sufficient for being involved in the case, triggering the duty to disclose evidence. This standard of relevance is much lower than the Dutch test, which often requires the applicant to convince the court that particular types of document or evidence are being kept under the requested party's management. Requesting as such especially is burdensome for victims of cyber violations who only have a limited amount of available evidence.
- A list of the requested documents and evidence shall be provided, and the applicant must explain its 'legitimate interest' in obtaining such data, for instance, for and only for strengthening a future claim against that particular wrongdoing. This condition, which is influenced by the Dutch concept, serves as a filter to deter applicants from abusing the right to disrupt the requested party. This listing request also obstructs 'fishing expedition' claims, which are typically attached with the British's 'full and frank' disclosure.
- The court shall consider the necessity and proportionality to approve such an application on a case-by-case basis. For the test of necessity, the applicant shall prove that seeking this decision is the last resort to obtain evidence as in the Dutch model at Article 843a DCCP. This is due to the immense potential impact of this decision on the violators' rights and the evidence holders' interests. If an alternative to collect evidence exists, such as witness examination (or the 'mere witness' exception in British law) or a reveal of newly available sources, the order should not be granted. This requirement does not prevent the victims of cyber violations from using the right, given they often have no other source than those kept by third parties like the online platforms or service providers. Regarding the proportionality test, the question to be asked is whether the importance of the requested evidence to the applicant might prevail against the violators' privacy and the confidentiality duty and other interests of the requested party. The factors incorporated in either British law (*RFU v Viagogo*) or Dutch law (Article 843a DCCP bracket i and ii) are valuable sources for improving this matter. In such a consideration, the court should be given a certain amount of discretion but shall explain their reasoning to ensure stability and legitimate expectations of all parties.

Third, regarding the scope of the disclosure, the applicant shall be requested to specify the documents containing the evidence sought. Although the British order to reveal 'full and frank' information might help victims find all identified or unidentified evidence in cyberspace, it may result in the surge of 'fishing expedition' claims. Besides, to comply with potential orders, firms conducting business online or telecommunication services have to invest resources in finding, managing, storing almost all of their data, which is a heavy burden for small and medium-sized companies

in a developing nation like Vietnam. Thus, similar to the Dutch concept, the applicant shall at least have some grounds to persuade the court that the evidence holders possess some relevant evidence. Additionally, this scope shall be free from other restrictions, as any data related to the wrongdoings and wrongdoers, including names, addresses, transaction details, correspondence, and others, shall be all disclosed if being listed in the request. The applicant shall be obligated to protect the obtained data under data protection laws, and applications from those having bad records on unlawful data use should be refused.

Finally, some particular procedures should be applied following the suggestions from the UK and the Dutch concepts. The applicant should not be forced to be a litigant after the disclosure, as the evidence sought might be unpersuasive for the applicant to confidently lodge a claim afterwards. Besides, the decision should be heard without notice to the violators but not the evidence holders. While there is a risk that the holders may instantly inform the wrongdoers in some cases, the evidence holders shall be allowed to defend their rights and interests at the court to balance the interests of the applicant. Additionally, the deadline for disclosure and penalty for non-compliance shall also be specified in this decision, similar to those of the Dutch courts, to prevent any obstruction or delay. The fixed 15 days time limit for a disclosure given by Article 106.3 CPC needs not to be similarly applied to this right. Given that a two-week waiting period might be too lengthy for the victims of cyber violations, the court should be freed to set a shorter deadline on a case-by-case basis.

CONCLUSION

In the technological era where an ordinary person usually spends one-fourth of a day on the Internet[35], legal issues and conflicts arising from online relations and transactions might shortly become undeniable parts of everyone's life. To control legal violations in cyberspace and secure the interests of victims, a prompt collection of adequate evidence from the third-party evidence holders is of paramount importance, and such an effort may not succeed without the aid of the public powers. The procedural laws of both the UK and the Netherlands, being integrated with specific mechanisms to support the victims in this crucial stage, have proven their effectiveness in several cases against cyber violations. By contrast, Vietnamese procedural law has not covered this issue thoroughly, leaving room for improvement. While incorporating a new and ambitious clause about preaction evidence collection to the CPC might be a current need, further in-depth research should also be taken to develop the best structure and procedures for such a mechanism.

LIST OF ABBREVIATIONS

CPC: Vietnamese Civil Procedure Code
UK: United Kingdom
DCCP: Dutch Code of Civil Procedure

CONFLICT OF INTEREST

The author hereby declares that there is no conflict of interest in the publication of this article.

AUTHORS' CONTRIBUTION

The entire content of the article is done by the author only.

REFERENCES

1. Le THX, Nguyen TTL. Cybercrime in the era of industrial revolution 4.0. Journal of the People's Court 2018;18;.
2. Tran AT. Scientific commentary on the Civil Procedure Code 2015. The Judicial Publisher; 2017;.
3. Hands v Morrison Construction Services Ltd [2006] Adj.L.R. 06/16. 2006;.
4. Marfe M. A pan-European guide to obtaining evidence. Managing Intellectual Property 2009:38;.
5. Mitsui & Co Ltd v Nexen Petroleum UK Ltd. 2005;.
6. Popplewell J. Orb A.R.L v. Fiddler. 2016;.
7. Golden Eye (International) Ltd v Telefonica UK Ltd. 2012;.
8. King J. Campaign Against Arms Trade v BAE Systems plc. 2007;.
9. Lord Reid. Norwich Pharmacal Co. v Commissioners of Customs and Excise. 1974;.
10. The Rugby Football Union v Consolidated Information Services Limited (formerly Viagogo Limited). 2012;.
11. British Steel Corporation v. Granada television Ltd. 1981;.
12. Bankers Trust Co v Shapira. 1980;.
13. LaRoche K, Pratte GJ. The Norwich Pharmacal Principle and Its Utility in Intellectual Property Litigation. Advocates' Quarterly 2001;24:301-25;.
14. G and G v. Wikimedia Foundation Inc. 2009;.
15. Coca Cola Company and Others v. British Telecommunications plc. 1998;.
16. Killen T, Clerk W. Practical guide to: Norwich Pharmacal orders. 2TG Commercial Fraud Team; 2018;.
17. UBT v. Moffitt. 2017;.
18. Supreme Court of the Netherlands (Hoge Raad). Shooting incident Alphen a / d Rijn (ECLI:NL:HR:2015:1834). 2016;.
19. The Hague District Court. ECLI:NL:RBSGR:2012:BX5675. 2012;.
20. Supreme Court of the Netherlands (Hoge Raad). Semtex v. Defendants (NL:HR:2020:1251). 2020;.
21. Zeri C, Mulder D. Confidential Information in Dutch IP Proceedings: From "Don't Ask, Don't Tell" to "Show and Tell." European Intellectual Property Review 2019:8;.
22. Supreme Court of the Netherlands (Hoge Raad). ECLI:NL:HR:2012:BW9244. 2012;.
23. Meerdink E. The Dispute Resolution Review: Netherlands. The Dispute Resolution Review. 13th ed., The Law Reviews; 2021;.
24. Amsterdam District Court. ECLI:NL:RBAMS:2012:BY2758. 2012;.
25. Amsterdam Court of Appeal. ECLI:NL:GHAMS:2008:BE2917. 2008;.
26. Gelderland District Court. ECLI:NL:RBGEL:2018:2828. 2018;.
27. Rotterdam District Court. Claimants v. Food for the Mind Holding BV (ECLI:NL:RBROT:2012:BY8336). 2012;.

28. Amsterdam District Court. ECLI:NL:RBAMS:2005:AU4935. 2005;.
29. The Attorney General at the Supreme Court of the Netherlands. Conclusion on Syngenta Seeds BV v. [defendant]. 2018;.
30. The Hague District Court. Turboned v. Wiandel Holding and defendants (ECLI:NL:RBSGR:2012:BX5675). 2012;.
31. Clever-ID v Defendant (ECLI:NL:RBARN:2010:BO3338). 2010;.
32. Jumbodiset BV v KPMG (ECLI:NL:RBAMS:2010:BP3071). 2010;.
33. Lockton Companies International & Ors v Persons Unknown & Anor. 2009;.
34. Applause Store Productions Ltd. & Anor v Raphael. 2008;.
35. Hootsuite, WeAreSocial. Digital 2019: Global digital overview. Datareportal; 2019;.

Tạp chí Phát triển Khoa học và Công nghệ – Kinh tế-Luật và Quản lý, 6(1):2175-2183

Open Access Full Text Article

Bài nghiên cứu

Hoàn thiện pháp luật Việt Nam về thu thập chứng cứ tiền tố tụng chống các hành vi phạm pháp trên không gian mạng

Đào Trọng Khôi[1,2,*]

Use your smartphone to scan this QR code and download this article

TÓM TẮT

Trong thời đại công nghệ hiện nay, các hành vi vi phạm pháp luật đang ngày càng gia tăng trên không gian mạng và gây ra những thiệt hại đáng kể, nhờ tận dụng sự nhanh chóng và tiện lợi của Internet khi kết nối và thực hiện các giao dịch trực tuyến. Điều kiện tiên quyết để nạn nhân của các hành vi phạm pháp kể trên sử dụng các công cụ pháp lý để bảo đảm quyền và lợi ích của mình là phải thu thập được đầy đủ bằng chứng và thông tin liên quan đến các hành vi đó. Hoạt động này phải được tiến hành sớm nhất có thể và thậm chí cần được thực hiện trước khi quá trình tố tụng bắt đầu, nhằm ngăn chặn việc các dữ liệu và thông tin quan trọng về thủ phạm bị tẩu tán hoặc xoá vĩnh viễn. Tuy nhiên, những dữ liệu này thường được lưu trữ bởi chính thủ phạm hoặc được đặt dưới sự quản lý của các bên thứ ba như mạng xã hội, nhà cung cấp dịch vụ Internet, hoặc ngân hàng. Các bên này có xu hướng từ chối yêu cầu tiết lộ các thông tin kể trên do có xung đột lợi ích, để đảm bảo bí mật khách hàng và tránh các rủi ro kinh doanh khác. Trước tình trạng kể trên, pháp luật tố tụng dân sự Việt Nam còn tồn tại một số vấn đề gây khó khăn cho người bị hại khi thu thập chứng cứ ở giai đoạn tiền tố tụng. Các quy định này chưa làm rõ quyền của người bị hại khi thu thập chứng cứ từ người nắm giữ, cũng như chưa có bất kỳ biện pháp hữu hiệu nào khác để hỗ trợ nạn nhân thu thập chứng cứ trong giai đoạn quan trọng này. Trong khi đó, luật tố tụng của một số quốc gia trên thế giới như Vương quốc Anh và Vương quốc Hà Lan tồn tại một số cơ chế hiệu quả để giải quyết vấn đề này. Về cơ bản, pháp luật Anh và Hà Lan cho phép nạn nhân yêu cầu tòa án ra lệnh cho người giữ các bằng chứng phải giao nộp các chứng cứ quan trọng về các vi phạm và thông tin về thủ phạm kể cả khi một vụ kiện dân sự chưa được thụ lý. Bằng phương pháp nghiên cứu luật viết (doctrinal) và phương pháp luật so sánh (comparative), bài viết phân tích kinh nghiệm quốc tế để xác định một số điểm quan trọng mà luật tố tụng dân sự Việt Nam cần tham khảo khi hoàn thiện các quy định về quyền yêu cầu tòa án hỗ trợ thu thập chứng cứ ở giai đoạn tiền tố tụng.

Từ khoá: Luật tố tụng, thu thập chứng cứ, vi phạm pháp luật, không gian mạng, tiền tố tụng

[1]*Khoa Kinh doanh, Đại học FPT Hà Nội, Việt Nam*

[2]*Khoa Luật, Đại học Quốc gia Hà Nội, Việt Nam*

Liên hệ

Đào Trọng Khôi, Khoa Kinh doanh, Đại học FPT Hà Nội, Việt Nam

Khoa Luật, Đại học Quốc gia Hà Nội, Việt Nam

Email: khoidt3@fe.edu.vn

Lịch sử

- Ngày nhận: 23-5-2021
- Ngày chấp nhận: 29-9-2021
- Ngày đăng: 25-12-2021

DOI : 10.32508/stdjelm.v6i1.832

Check for updates

VNU-HCM Press

Trích dẫn bài báo này: Khôi D T. **Hoàn thiện pháp luật Việt Nam về thu thập chứng cứ tiền tố tụng chống các hành vi phạm pháp trên không gian mạng**. *Sci. Tech. Dev. J. - Eco. Law Manag.;* 6(1):2175-2183.