Title: **Electronic Evidence in Civil and Commercial Dispute Resolution: A Comparative Perspective of UNCITRAL, the European Union, Germany and Vietnam**

Author: **Quynh Anh Tran**

Date and place of publication: **2022, Switzerland**

Publisher: **Springer Nature Switzerland AG**

ISBN hardback: **978-3-031-18571-7**

ISBN eBook: **978-3-031-18572-4**

After a high-level introductory chapter, in which the author sets the scene in the context of the rise of the internet (although evidence in electronic form was reaching the courts in the 1960s, for which see p 81), and sets out the content of each chapter, the author provides a useful and detailed resume of the position regarding electronic evidence in the context of UNCITRAL and the European Union in chapter 2. Although neither UNCITRAL nor the European Union has produced a specific text on electronic evidence to date, both organizations have produced a significant number of provisions that addresses some issues specifically (e.g., electronic signatures; admission of evidence in electronic form) that help to ensure evidence in electronic form is not considered to be inferior to evidence in any other form.

The second part of chapter 2 (2.3), the author sets out the legal framework of Germany (indicating that the eIDAS Regulation finally resolved the inconsistency of German law (p 24), followed by the legal framework of Vietnam (2.4), which was influenced and altered by the French colonial authorities before significant changes began to be effected by reforms, called the Renovation Period, beginning in 1986 (p 28). Dr Tran concludes this chapter with the observation (p 35), that although German law contains many provisions relevant to evidence in electronic form, they are not as precise as in other countries, such as Austria. At present, the author points out that 'Vietnam has tried to enact legislation on the use of information technology and electronic evidence in arbitral and civil proceedings. However, the Vietnamese legal system is not systematic and too complicated, which creates many difficulties for the involved parties, the lawyers and also the Vietnamese courts.'

Disclosure (or discovery) of evidence in legal proceedings is crucial, as the English legal system has discovered from the Post Office Horizon scandal, which has been the worst legal scandal in centuries, caused by the failure to order appropriate disclosure of electronic evidence.[1] In setting out principles in chapter 3, 'Fundamental Principles of Civil Procedure and the Basic Principles Relating to Evidence in Civil Procedure', Dr Tran observes (p 40) that 'After receiving suggestions from the German court, the parties have the right to decide whether they will produce further information or not. In case they determine not to do so, the court shall be bound by only the presented facts to solve the case (Sec. 139(1) ZPO).' Dr Tran also notes that 'the court has authority to order evidence on its own motion in certain cases.'

As chapter 9 deals with the evaluation of electronic evidence and the burden of proof (pp 233 – 247), it will have been of substantial interest to be given guidance, including case law, of the topic of disclosure (or discovery) of evidence in each of the situations covered in the text. This is important, given just one example of a failure, where

[1] For a brief chronology of the Post Office Horizon legal scandal, see https://journals.sas.ac.uk/deeslr/article/view/5390.

the Post office in England and Wales failed to disclose relevant evidence in the prosecution of Seema Misra, and was not ordered to provide disclosure by three judges.[2] The simple fact is, that data in electronic form now forms the majority of evidence in cases brought before the courts in every jurisdiction in the world. If a party has the ability to determine what evidence it wishes to adduce in legal proceedings, and a judge does not enforce the disclosure of relevant electronic evidence, miscarriages of justice will already have taken place across the globe and will continue to do so unless this topic is satisfactorily resolved.

It will have been of great interest for Dr Tran to have dealt with this crucially important issue with more research – if, that is, the jurisdictions chosen for this work were open about this particular fundamental issue.

Chapter 4, 'Basic Issues of Evidence and Electronic Evidence in Civil and Commercial Dispute Resolution' provides a high-level discussion of the basic principles relating to evidence, such as the concept, relevance and admissibility; discussions of the types of evidence available and expert witnesses. Evidence in electronic form is discussed at 4.2, including a detailed discussion of the definitions and an outline of the characteristics of electronic evidence. A brief introduction is given to how digital devices work and how devices connect (pp 81 – 86).

In chapter 5, Dr Tran covers the basic concepts of 'document' and other forms of document in electronic form such as email, SMS and IM, audio and video recordings, data from the internet (e.g., web sites, social networking). Following on, in chapter 6, consideration is given to finding and the subsequent analysis (including the provisions of expert reports) of evidence in electronic form, including the requirement for specialist help to recover evidence in a form that can be proven to have a continuity of careful handling, and that is it appropriately preserved, otherwise the evidence is open to being undermined for not being appropriately authentic. This chapter also considers the implications relating to personal data.

Chapter 7 considers the authenticity of evidence in electronic form. The topic is introduced at pp 167 – 175, which is followed by a discussion of electronic signatures at 7.2, and the position regarding manuscript signatures in Vietnam and Germany is set out at page 178. Some German case law is usefully discussed at pp 178 – 181. Electronic

[2] The transcript of the trial of *Regina v Seema Misra*, T20090070, in the Crown Court at Guilford, Trial dates: 11, 12, 13, 14, 15, 18, 19, 20, 21 October and 11 November 2010, His Honour Judge N. A. Stewart and a jury, was published in full in (2015) 12 *Digital Evidence and Electronic Signature Law Review*, Introduction 44; Documents Supplement, available at https://journals.sas.ac.uk/deeslr/issue/view/328; see also Tim McCormack, 'The Post Office Horizon system and Seema Misra' (2016) 13 *Digital Evidence and Electronic Signature Law Review* 133, available at https://journals.sas.ac.uk/deeslr/article/view/2303. In this case, the prosecuting barrister referred to the Horizon system being 'robust' – seemingly in an attempt to refer to the presumption that computers are reliable without actually committing to using the word 'reliable', for which see Peter Bernard Ladkin, Bev Littlewood, Harold Thimbleby and Martyn Thomas CBE, 'The Law Commission presumption concerning the dependability of computer evidence', (2020) 17 *Digital Evidence and Electronic Signature Law Review* 1, available at https://journals.sas.ac.uk/deeslr/article/view/5143; Peter Bernard Ladkin, 'Robustness of software', (2020) 17 *Digital Evidence and Electronic Signature Law Review* 15, available at https://journals.sas.ac.uk/deeslr/article/view/5171; Michael Jackson, 'An approach to the judicial evaluation of evidence from computers and computer systems' (2021) 18 *Digital Evidence and Electronic Signature Law Review* 50, available at https://journals.sas.ac.uk/deeslr/article/view/5289; for a discussion of the evidence the Post Office ought to have disclosed before trial, see James Christie, 'The Post Office Horizon IT scandal and the presumption of the dependability of computer evidence' (2020) 17 *Digital Evidence and Electronic Signature Law Review* 49, available at https://journals.sas.ac.uk/deeslr/article/view/5226. The disclosure of relevant digital data was a live issue in this case. The defence made a number of requests for further disclosure of the computer system. This was refused 4 times: first application before Mr Recorder Bruce, 10 March 2010 (Day 1 Monday 11 October 2010, 3C; Judge's Ruling, Day 1 Monday 11 October 2010, 25, A-C); second application before HH Judge Critchlow, 7 May 2010 (Day 1 Monday 11 October 2010, 3G); third application before the trial judge (Day 1 Monday 11 October 2010, 15H-16H) and fourth application before the trial judge (Day 6, Monday 18 October 2010, 24H-25A) – on this precise point, see *Hamilton v Post Office Ltd* [2021] EWCA Crim 577 at [204], available at https://www.bailii.org/ew/cases/EWCA/Crim/2021/577.html.

signatures under the UNCITRAL legal texts are set out at pp 181 – 185, and the EU Directive and Regulation are covered at 7.2.3. Dr Tran considers the nature of the 'advanced electronic signature' and the debate, concluding, at p 188:

> 'From my perspective, an advanced electronic signature is made and retained by the technical program on the diital devices under the control of the signatory. Theoretically, the advanced electronic signature is unique and linked to the signatory because it was made and used intentionally on his purpose. Nevertheless, the signatory cannot remember the complex information of his own electronic signature, particularly with regard to the evolution of information technology, the advanced electronic signature shall be more and more complicated. Moreover, it is possible that the third party uses his advanced electronic signature with or without his knowledge and permission. The requirement that an advanced electronic signature is uniquely linked to the signatory, therefore, is more or less hypothetical. This is due to the different characteristics of the advanced electronic signature to the manuscript signature.'

The problem with the observation by Dr Tran that the 'requirement that an advanced electronic signature is uniquely linked to the signatory, therefore, is more or less hypothetical' is that a number of jurisdictions have also enacted legislation providing a link to the signatory that is impossible. The link to the signatory is not possible, as demonstrated by the nature of the private key. An example of a private Exponent is illustrated below:[3]

Private Exponent:

5c:a2:77:1b:6a:45:0c:af:e4:aa:c3:91:b2:7e:ab:

ea:ec:27:14:25:6a:2a:67:d8:ce:25:1a:e4:09:11:

f2:31:10:b1:43:c9:dd:d7:a7:13:d7:14:21:91:c5:

15:27:ff:cd:8d:64:d5:e5:3e:64:48:a2:95:ec:d9:

3f:75:8e:22:d9:11:42:90:c3:e9:fb:de:3d:ba:69:

d4:db:b5:eb:84:68:f1:92:ad:36:71:04:b4:4a:f6:

03:2f:5f:6c:ac:b0:ed:30:5a:89:94:c8:82:ea:55:

eb:62:e8:09:0b:d0:d2:40:b8:a7:2e:70:71:aa:59:

58:14:21:ae:20:d6:16:84:d2:29:5c:9b:a7:56:50:

3a:10:0b:c6:70:2b:97:dd:f8:fa:73:74:22:5f:d6:

ce:0d:75:45:8a:61:5d:86:25:cb:ad:19:06:fe:8e:

a4:f9:0d:35:2a:02:04:93:ec:df:0c:db:ca:f0:8c:

ae:a7:54:c2:37:a1:11:7b:9f:40:54:a4:fd:31:a4:

f9:ee:60:3c:8f:3b:0e:b1:e2:10:6d:f0:36:50:63:

27:6e:cc:85:c1:5d:10:4a:36:23:5d:bf:c7:ee:9b:

af:3f:e6:49:47:c6:9e:b8:00:b0:d9:d2:de:07:46:

[3] This example is from Symeon (Simos) Xenitellis, 'The Open–source PKI Book: A Guide to PKIs and Open–source Implementations' and quoted under GNU Free Documentation License, Version 1.3, 3 November 2008 published by the Free Software Foundation: http://ospkibook.sourceforge.net/docs/OSPKI-2.4.7/OSPKI-html/sample-key-components.htm.

43:14:2f:de:7c:51:57:a5:8d:4b:13:04:54:25:3b:

d5

This example services to illustrate the point that committing the private key to memory is impossible (with the exception of a very few individuals), which is why the legal presumption that an advanced electronic signature is uniquely linked to the signatory is an impossibility.

The position regarding electronic signatures under Vietnam law is considered at 7.2.4 (pp 189 – 192), and a general overview of authentication of various data in electronic form is discussed at 7.3 (e.g., emails, web sites, etc). Readers familiar with common law will be surprised that under German law, only emails which contained a qualified signature may be considered as formally effective (p 199).[4] Dr Tran suggests, at 7.4 in her Interim Conclusion, that 'electronic evidence must be authenticated in order to be admitted before the courts or arbitral tribunals.' This, of course, is particular to specific jurisdictions. Where evidence is agreed between the parties (as in civil proceedings in England and Wales, where there is a procedural rule by which parties have to challenge the authenticity of evidence before trial, otherwise the parties accept the authenticity of the evidence the other party intends to adduce, thus reducing the costs of the trial), there is no need to go to the expense of authentication if authentication is not at issue.

At p 209, Dr Tran highlights the failure of the legal profession to educate judges and lawyers:

> 'Even though electronic evidence is presented more and more in civil and arbitral proceedings, the courts and arbitral tribunals are still facing difficulties in deciding the authenticity of electronic evidence because they are unfamiliar with the new information technology. … To successfully deal with electronic evidence, the legal experts, the courts and arbitral tribunals must enhance their knowledge of information technology.'

This journal was set up partly for that purpose, and has consistently called for legal education, without success.[5]

Dr Tran also suggests:

[4] For relevant early German case law translated into English, see: OLG Köln, 19 U 16/02; LG Konstanz, 2 O 141/01 A; AG Erfurt, 28 C 2354/01, (*Evidential value of declarations sent by e-mail*), reported by Michael Knopp, Researcher at provet, University of Kassel, Germany, 2 *Digital Evidence and Electronic Signature Law Review* (2005) 105 – 106, available at https://journals.sas.ac.uk/deeslr/article/view/1760; Case Note, Germany: 10 A 11741/05 (*Procedure; time limits; Administrative Court; need for qualified electronic signature*), commentary by Dr Martin Eßer , 4 *Digital Evidence and Electronic Signature Law Review* (2007) 91 – 92, available at https://journals.sas.ac.uk/deeslr/article/view/1807; Germany, Case Translation: 12 U 34/07, Court of Appeal Berlin (Kammergericht Berlin), 30 August 2007, commentary by Dr Martin Eßer, (*Private electronic documents; 'instrument'; qualified electronic signature*), 5 *Digital Evidence and Electronic Signature Law Review* (2008) 110 – 111, available at https://journals.sas.ac.uk/deeslr/article/view/1834; Case Translation, Germany: 22.09.2009, 1 K 365/09.TR, commentary by Dr Martin Eßer, (*Right to appeal; electronic means; administrative proceedings*), 7 *Digital Evidence and Electronic Signature Law Review* (2010) 156 – 157, available at https://journals.sas.ac.uk/deeslr/article/view/1834.

[5] Calls for education: Editorial, 4 *Digital Evidence and Electronic Signature Law Review* 2007; Editorial, 7 *Digital Evidence and Electronic Signature Law Review* 2010; Editorial, 9 *Digital Evidence and Electronic Signature Law Review* 2012 – particularly pertinent; Editorial, 10 *Digital Evidence and Electronic Signature Law Review* 2013 [including a free syllabus]; Denise H Wong, 'Educating for the future: teaching evidence in the technological age' (2013) 10 *Digital Evidence and Electronic Signature Law Review* 16; Deveral Capps, 'Fitting a quart into a pint pot: the legal curriculum and meeting the requirements of practice' (2013) 10 *Digital Evidence and Electronic Signature Law Review* 23, both articles available at https://journals.sas.ac.uk/deeslr/issue/view/310; Editorial, 13 *Digital Evidence and Electronic Signature Law Review* 2016; Editorial, 17 *Digital Evidence and Electronic Signature Law Review* 2020.

> ‘Therefore, it is a desire to harmonize the legal framework relating to the use of electronic evidence within the EU, which should start with common guidance or standards to authenticate electronic evidence in civil proceedings.’

This suggestion is of great interest. It is a pity that Dr Tran did not discuss the *Draft Convention on Electronic Evidence* in this context.[6]

The admissibility of evidence in electronic form is considered in chapter 8, and Dr Tran discusses relevant case law in the context of the European Union (p 213), and the criteria for admission is further discussed (pp 214 – 217) before considering the difficulties in assessing evidence in electronic form (p 217 – 218). Illegally obtained evidence and admissibility follows (pp 218 – 230), which canvasses a wide range of relevant case law and the opinions of legal commentators.

Chapter 10 provides a list of suggestions for the future, which comprise issues relating to evidence, and a mix of other, related issues, including procedure, the development of an IT infrastructure for the courts and other miscellaneous matters, as set out on p 281 in the Final Conclusion, chapter 11:

> ‘From the author’s perspective, further researches should be done on the following matters:
>
> 1. The implementation of the current laws on the use of electronic evidence in civil and/or arbitral proceedings
>
> 2. The proposed provisions on electronic evidence as a part of the Europeanisation of civil procedure
>
> 3. Taking of electronic evidence in cross-border cases within the EU
>
> 4. Authentication and admission of electronic evidence in cross-border cases in the EU
>
> 5. Enhancing the use of information technology in modern court and/or arbitration
>
> 6. The detailed analysis on the electronic signature regime as a way of authentication of electronic evidence
>
> 7. The guidance to electronic evidence discovery relating to the up-to-date technology
>
> 8. The protection of fundamental rights in data investigation, or
>
> 9. Generally, legal issues of transnational taking of electronic evidence’

This book is clearly the result of Dr Tran’s doctorate. It reads and is structured like a doctorate. This is where the publishers have failed the author and reader. The content is important and useful to the lawyer, but the publishers should have appointed an editor to help Dr Tran restructure her doctorate into a more useable text for the practicing lawyer.

Notwithstanding the lack of discussion about what can be described as the most fundamental aspect of electronic evidence in legal proceedings of all kinds – the disclosure or discovery of evidence – this is a useful text that has added to the understanding of evidence in electronic form across UNCITRAL, the European Union, Germany, and Vietnam.

Comparative texts can be useful, but unfortunately, practicing lawyers will prefer a text covering their own jurisdiction in isolation. This is a practical point that does not derogate from Dr Tran’s achievement. This highlights the difficulty of the author attempting to provide a text that guides lawyers and judges in electronic evidence: the technical issues relating to electronic evidence remain the same for all jurisdictions, but the legal framework differs – hence a comparative study, as good as it is, can never fully compensate for a book that covers a single jurisdiction.

[6] Available at https://journals.sas.ac.uk/deeslr/article/view/2321.

Perhaps Dr Tran will consider a jurisdiction-only text for one of the jurisdictions set out this this book in due course. If not, then Dr Tran has provided a good overview for future authors of such practitioner texts.

Contents