“Reliable System” in English Law and Reliable Systems

Peter Bernard Ladkin
20250130

Paper documents with legal meaning in business and trade are being replaced by documents generated by and held on digital computer systems; in short, electronic documents. The Electronic Trade Documents Act 2023[1] defines what is to count as an electronic trade document for the purposes of the law of England and Wales. Section 2 defines “electronic trade document”[2]:

> *(1) This section applies where information in electronic form is information that, if contained in a document in paper form, would lead to the document being a paper trade document.*
>
> *(2) The information, together with any other information with which it is logically associated that is also in electronic form, constitutes an “electronic trade document” for the purposes of this Act if a reliable system is used to –*
>
> *(a) identify the document so that it can be distinguished from any copies,*
> *(b) protect the document against unauthorised alteration,*
> *(c) secure that it is not possible for more than one person to exercise control of the document at any one time,*
> *(d) allow any person who is able to exercise control of the document to demonstrate that the person is able to do so, and*
> *(e) secure that a transfer of the document has effect to deprive any person who was able to exercise control of the document immediately before the transfer of the ability to do so (unless the person is able to exercise control by virtue of being a transferee).*
>
> *(3) For the purposes of subsection (2) –*
>
> *(a) a person exercises control of a document when the person uses, transfers or otherwise disposes of the document (whether or not the person has a legal right to do so), and*
> *(b) persons acting jointly are to be treated as one person.*
>
> *(4) Reading or viewing a document is not, of itself, sufficient to amount to use of the document for the purposes of subsection (3)(a) –*
>
> *(5) When determining whether a system is reliable for the purposes of subsection (2), the matters that may be taken into account include –*
>
> *(a) any rules of the system that apply to its operation;*
> *(b) any measures taken to secure the integrity of information held on the system;*
> *(c) any measures taken to prevent unauthorised access to and use of the system;*

1 https://bills.parliament.uk/bills/3344
2 https://www.legislation.gov.uk/ukpga/2023/38/section/2/enacted

(d) the security of the hardware and software used by the system;
(e) the regularity of and extent of any audit of the system by an independent body;
(f) any assessment of the reliability of the system made by a body with supervisory or regulatory functions;
(g) the provisions of any voluntary scheme or industry standard that apply in relation to the system.

Subsection (2) introduces the notion of "reliable system" and subsection (5) gives the conditions which are to be assessed when determining if a system is reliable. It follows that "reliable system", meaning reliable digital computational system, is since 2023 a concept of English law.

The issue of when and how one can depend upon a digital computational system, here for producing and managing trade documents, has been in English law for some forty years. The Police and Criminal Evidence Act (PACE) 1984 section 69 subsection (1) regulates *Evidence from computer records*[3]

(1) In any proceedings, a statement in a document produced by a computer shall not be admissible as evidence of any fact stated therein unless it is shown –
(a) that there are no reasonable grounds for believing that the statement is inaccurate because of improper use of the computer; ,
(b) that at all material times the computer was operating properly, or if not, that any respect in which it was not operating properly or was out of operation was not such as to affect the production of the document or the accuracy of its contents ; and
(c) that any relevant conditions specified in rules of court under subsection (2) below are satisfied.

[Subsection 2 omitted]

Subsection (1)(b) was particularly onerous. It had to be shown that at all material times the computer was operating "properly". Notoriously, digital computers don't always do "the right thing" or produce the "right output". The Law Commission considered this burden in a 1997 report[4] and recommended PACE S. 69 be repealed, in favour of the common law presumption (the Presumption) that a digital computer, like a mechanical devices, could be presumed by the courts to be operating "properly" at the material time unless there was evidence that it wasn't. I and colleagues have discussed the Presumption in 2020[5] and found it significantly wanting[6].

---

3 https://www.legislation.gov.uk/ukpga/1984/60/section/69/enacted
4 The Law Commission, Evidence in Criminal Proceedings: Hearsay and Related Topics (1997), available from https://lawcom.gov.uk/project/evidence-in-criminal-procedings-hearsay/#related
5 Ladkin, P.B., Littlewood, B., Thimbleby, H.W., Thomas, M., The Law Commission presumption concerning the reliability of computer evidence, Digital Evidence and Electronic Signature Law Review 17 (2020), available from https://journals.sas.ac.uk/deeslr/article/view/5143
6 See also James Christie, The Post Office Horizon IT scandal and the presumption of the dependability of computer evidence, Digital Evidence and Electronic Signature Law Review 17 (2020), available from https://journals.sas.ac.uk/deeslr/article/view/5226 and also James Christie, The Law Commission and section 69 of the Police and Criminal Evidence Act 1984, Digital Evidence and Electronic Signature Law Review 20 (2023), available from https://journals.sas.ac.uk/deeslr/article/view/5642

The barrister Paul Marshall was approached by the UK Ministry of Justice in 2020 with a request to suggest what procedures (short of reinstating PACE 1984 S. 69) would be appropriate for assessing the probity of computer evidence presented to the courts. He consulted software reliability experts (amongst them myself) and our recommendations were sent to the Ministrat, and then were published in 2021, with a further synopsis in 2022[7]

The UK government issued on 21st January 2025 a Call for Evidence about modifying the Presumption in criminal proceedings[8].

There is a difference between the recommendations for probity of computer evidence given in Marshall et al. 2020, and the notion of what counts to establish a "reliable system" in ETDA 2023. One can imagine that this might have to do with the different standards of proof in civil cases (balance of probabilities) and criminal cases (beyond reasonable doubt).

However, the notion of "reliable system" has a much longer provenance than ETDA 2023. There is a branch of software engineering called "software reliability" and its subject matter has been established for decades. The US Institute of Electrical and Electronics Engineers (IEEE), since 1963 the US professional society for electrical engineering, and a major issuer of standards which are often adopted internationally by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC, responsible for international standards in electrotechnology) defined "reliability", of systems, up to 1990[9], thus:

> ***reliability.*** *The ability of a system or component to perform its required functions under stated conditions for a specified period of time.*

The IEC defines "reliability" in the International Electrotechnical Vocabulary (IEV) thus[10]:

> ***reliability***
>
> *ability to perform as required, without failure, for a given time interval, under given conditions*

These definitions are all but identical in meaning, as might be expected from a mature engineering discipline. Note, though, that the IEV definition applies to all equipment associated with electrotechnology, not just software.

The IEC also admits a notion of quantified reliability, in the third note to the above entry[11]:

---

7 Marshall, P., Christie, J., Ladkin, P.B., Littlewood, B., Mason, S., Newby, M., Rogers, J., Thimbleby, H.W. Thomas, M., Recommendations for the probity of computer evidence, Digital Evidence and Electronic Signature Law Review 18 (2021), available from https://journals.sas.ac.uk/deeslr/article/view/5240 ; and for the synopsis Bohm, N., Christie, J., Ladkin, P.B., Littlewood, B., Marshall, P., Mason, S., Newby, M., Rogers, J., Thimbleby, H.W. Thomas, M., Briefing Note: The legal rule that computers are presumed to be operating correctly – unforeseen and unjust consequences, Digital Evidence and Electronic Signature Law Review 19 (2022), available from https://journals.sas.ac.uk/deeslr/article/view/5476

8 Press Release at https://www.gov.uk/government/news/use-of-computer-evidence-in-court-to-be-interrogated , Call for Evidence at https://www.gov.uk/government/calls-for-evidence/use-of-evidence-generated-by-software-in-criminal-proceedings

9 IEEE Standard Glossary of Software Engineering Terminology, IEEE Std. 610.12-1990, IEEE 1990.

10 https://www.electropedia.org/iev/iev.nsf/display?openform&ievref=192-01-24

11 https://www.electropedia.org/iev/iev.nsf/display?openform&ievref=192-01-24

Note 3 to entry: Reliability can be quantified using measures defined in Section 192-05, *Reliability related concepts: measures*.

This provision is taken by those working in "software reliability" to be essential. As noted by Christie[12], computer hardware has different reliability properties than computer software and computer data. It is generally agreed amongst software reliability experts that most non-trivial software has "bugs", ways in which it works that lead to different outcomes than desired ("failures"). In terms of the black-and-white definition of reliability, this would entail that most non-trivial software is not "reliable", rendering this concept unhelpful in the analysis of software. Quantifying "reliability" for software allows that, under a certain "operational profile" (a given collection of inputs and their relative frequencies) the proportion of successes and failures of the software on this profile may be statistically evaluated; indeed, this approach is the subject of most technical conferences and publications in the field of software reliability.

Notice that here we are talking about what it is for a system to be reliable. We are not talking about what it is for data to be reliable, or for evidence to be reliable, or for people to be reliable.

According to the IEV 192-01-24 definition (I take the IEEE and IEC definitions to have identical meaning, even though their syntax varies), a *reliable system* is one which performs as required, without failure, for a given time interval, under given conditions. This looks very much like what PACE 1984 S. 69 was requiring for use of electronic evidence in criminal court. And it doesn't look at all like what ETDA 2023 S. 2 is requiring.

What is to be done? Reliability is one of the central concepts in software engineering. One can foresee a different definition of "reliable system" in English law leading to difficulties in communication, and indeed to confusing points in argument[13].

A solution seems to be to be simple. There are two possibilities. The first is to distinguish the two notions explicitly when using them, e.g.:

- "reliable in the IEV sense"
- "reliable in the sense of ETDA 2023"

but these locutions are cumbersome.

The second is to distinguish through the property itself, as follows. A *reliable system* is what it has been for decades to engineers. The legal conditions, whether those established for civil cases in ETDA 2023 S. 2 or those to be established by Act of Parliament subsequent to the Call for Evidence opened on 21st January 2025 for criminal cases (and maybe civil cases as well), establish what the

12 James Christie, The Law Commission and section 69 of the Police and Criminal Evidence Act 1984, Digital Evidence and Electronic Signature Law Review 20 (2023), available from https://journals.sas.ac.uk/deeslr/article/view/5642

13 For example, in the form of argument presented by the prosecutor Mr. Tatford in R v Misra (Seema). See Case Transcript: England & Wales - Regina v Seema Misra, T20090070 - Commentary and Index to the transcript by Stephen Mason, in Digital Evidence and Electronic Signature Law Review 12 (2015), available from https://journals.sas.ac.uk/deeslr/article/view/2217 Mr. Tatford's argument has been considered in Ladkin, P.B., Robustness of software, Digital Evidence and Electronic Signature Law Review 17 (2020), available from https://journals.sas.ac.uk/deeslr/article/view/5171 James Christie has considered reliability in detail, as it refers to computer hardware, computer software, computer data, in James Christie, The Law Commission and section 69 of the Police and Criminal Evidence Act 1984, Digital Evidence and Electronic Signature Law Review 20 (2023), available from https://journals.sas.ac.uk/deeslr/article/view/5642

courts *take to be reliable* for legal purposes. This simple change of terminology indicates the difference quite precisely.

- "*reliable*" means what the IEV says;
- A system can be *taken to be reliable* by the courts using the criteria set out/to be set out in ETDA 2023. Or by lawmaking in response to the Call for Evidence.

Note that this solution has the advantage that the ETDA 2023 concept is clearly rebuttable. A system may be taken to be reliable using criteria explicated in ETDA 2023, but that doesn't mean the system is reliable; neither does it mean that the electronic trade document in question, for example a contract, can be relied upon by a court[14].

I can envisage a change in wording to ETCA 2023 to be worthwhile, from "*reliable system*" to "*system taken to be reliable*". This of course is up to lawyers and lawmakers.

14 Indeed, I was worried about this recently. A large UK shipping company filed a claim with Northampton County Court for unpaid invoices against my UK company. My company has never done any business with the shipping company. Somebody had established an account with them using the name and Registered Office address of my company and billed some goods shipping to it. I was worried for some time that they might also have faked a contract. To my relief, it seems not. The court claim was dropped.