Use of evidence generated by software in criminal proceedings: Call for Evidence

Response: By Dr. Micheál Ó Floinn (University of Glasgow) and Professor David Ormerod CBE, KC (UCL)

15th April 2025.

Questions:

1) The current common law (rebuttable) presumption is that computers producing evidence were operating correctly at the material time.

(a) Is this presumption fit for purpose in modern criminal prosecutions?

The presumption is not fit for purpose in modern criminal prosecutions.

(i) Please specify why you gave this answer

The presumption as it currently operates is fundamentally flawed as it presumes matters without adequate justification or scientific basis. This carries with it a significant risk of miscarriages of justice. We also find the presumption to be ambiguous in its defining features. The extension to 'computers' has never been adequately appraised or justified, either by the courts or by the Law Commission when it initially suggested that s. 69 PACE should be repealed and replaced with the 'presumption of proper functioning' of computers. In particular, we contend that the following matters are unclear as a matter of domestic law:

- Whether it comprises the well-established presumption of 'regularity', or a distinct presumption and, if the latter, what is the relationship with the *omnia praesumuntur rite esse acta* presumption? It is treated as such in *R v Shephard* [1993] A.C. 380, 384 Lord Griffiths, *Scott v Baker* [1969] 1 Q.B. 659, 675 Lord Parker CJ, *R v Skegness Magistrates' Court Ex p. Cardy* [1985] R.T.R. 49, 56 Robert Goff LJ. Compare, however, cases like *Castle v. Cross* [1985] 1 All E.R. 87, 89 *per* Stephen Brown L.J. (suggesting it is distinct but serves the 'same purpose' as *omnia praesumuntur rite esse acta*) and cases like *R. v Minors* (1989) 89 Cr. App. R. 102, 108 (where it is treated as a 'common sense inference').
- Whether 'proof of a basic fact' is required – by the party seeking admission of the evidence – for the presumption to even operate (e.g. that a mechanical instrument belongs to a category of instruments that are 'more often than not in working order'). Again, caselaw and evidence textbooks from the UK suggest different answers to this, and it is a fundamental issue which, we suspect, is not given sufficient consideration in the criminal courts.
- What is actually being presumed: is it that the instrument was '*in order when used*' (see e.g. *Castle v Cross* [1985] 1 All E.R. 87 , 89; *R v Skegness Magistrates' Court Ex p. Cardy* [1985] R.T.R. 49; *R v Spiby* (1990) 91 Cr. App. R. 186); that it was *'reliable'* (see *Cracknell v Willis* [1988] AC 450, 467; *Ali v DPP* [2020] 4 W.L.R.

146); that it was '*working correctly*' or in '*good working order'* (*Anderton v Waring* [1986] RTR 74, 80; *R v Shephard* [1993] A.C. 380, 384). Or only that a particular device was properly set or calibrated? (s. 129(2) Criminal Justice Act 2003).

- The nature of the relationship between the common law presumption(s) and s. 129(2) of the CJA 2003. Section 129(2) was said to 'preserve' the common law presumption (Explanatory Notes para 432), but the latter is seemingly much broader in practice.
- Issues continue to arise in relation to the type of burden (legal or evidential) that is placed on the defence through the operation of the presumption (see *Ali v DPP* [2020] EWHC 2864 (Admin) for recent consideration). We believe there is still uncertainty on the legal position where the defence seek to adduce 'computer evidence', and whether D bears a *legal* burden to prove the reliability/integrity/functioning etc of the computer(s) and their outputs if the presumption is challenged by the prosecution. The Law Commission previously suggested D would bear a legal burden to prove 'on the balance of probabilities' if there was some evidence led that "the computer was not working properly".[1] This is an area that is likely to generate Article 6 ECHR challenges in the future.

Ultimately, we would contend that the presumption rests on shaky foundations in English law. Key cases that are cited to support the existence of the presumption in *Castle v Cross* (eg *Nicholas v Penny* [1950] 2 KB 466; *Tingle Jacobs & Co v Kennedy* [1964] 1 ALL ER 888) have been overstated. Its extension to computer software (as opposed to mechanical instruments and hardware) has occurred uncritically and seemingly as an accident of history. And some of the few safeguards which were in-built in the presumption in its early forms were lost in caselaw without explanation or justification. See, for example, the approach of Stephen Brown LJ in *Castle v Cross,* following *Phipson* over *Cross on Evidence,* regarding whether the party relying on the presumption needed to prove a basic fact or not (e.g. that the instrument was 'of a kind as to which it is common knowledge that they are more often than not in working order') for the presumption to operate.

There is a lack of empirical evidence available as to how the presumption(s) is operating in practice, but we suspect there is significant risk of miscarriages of justice due to its operation in the modern criminal trial.

(b) How easy or difficult do you believe it is at present for this presumption to be effectively rebutted?

This is obviously a context-specific consideration. Clearly, there can be difficulties in rebutting the presumption if the objecting party is not privy to the processes that have

[1] Law Commission, *Evidence in Criminal Proceedings: Hearsay and Related Topics* (1997) (Law Com no 245), para 13.14.

been involved in gathering the evidence, and/or the party does not have access to relevant devices – and their outputs – to interrogate them. Therefore, whether the presumption can be rebutted will often hinge on the operation of disclosure rules, which has been before the courts on many occasions with respect to breathalyser machines. See e.g. *DPP v Manchester and Salford Magistrates' Court* [2017] EWHC 3719 (Admin); *DPP v Walsall Magistrates' Court* [2019] EWHC 3317 (Admin); R. *(on the application of DPP) v Caernarfon Crown Court* [2019] EWHC 767 (Admin). It is not difficult to imagine problems for an accused person in challenging a presumption in relation to the operation of more complex computers, when disclosure of relevant exculpatory evidence is not available, or known by prosecuting authorities.

Some cases may appear to suggest that the presumption is readily rebutted (see e.g. *DPP v Marrable* [2020] EWHC 566 (Admin), [15]). We would not accept that this is reflective of the usual process in the criminal trial. In *Marrable* itself, the admissibility of the defence evidence was not challenged by the prosecution (*ibid,* [16]). If it had been, the outcome in that case may well have been different.

The ease of rebuttal will also depend on the nature of the burden (legal or evidential) that is imposed on the party challenging the presumption (see above).

(c) What barriers do you see in effectively rebutting this presumption?

- Insufficient disclosure and availability of relevant evidence for rebuttal
- The complexity of modern computer systems.
- Uncritical acceptance of computer-generated evidence by trial counsel and judges/magistrates.
- Extraterritoriality in the evidence chain, where some of the entities and computers involved in capturing evidence are in other jurisdictions and not amenable to requests or orders from domestic courts.
- Availability of competent experts
- Costs and funding of appropriate experts

(i) Please give examples where possible.

See caselaw above related to disclosure and, of course, the *Post Office Horizon* cases also revealed widespread failures by Post Office Ltd in disclosing the faults in the Horizon software.

2) Are you able to provide examples from other jurisdictions or situations where the reliability of software must be certified?:

Canada and the Commonwealth Model law on Electronic Evidence

The Commonwealth Model law on Electronic Evidence contains a provision for proof by affidavit of matters related to e.g. the best evidence rule, and the presumption of integrity. This structure derives from the Canada Evidence Act 1985 (sections 31.1-31.8) and the Model law has been transposed domestically in a number of Commonwealth countries. In 2019 the Commonwealth Secretariat commissioned a review of the Model Law. This was undertaken by Dr. Ó Floinn (the document can be shared if needed, pending permission from the Commonwealth Secretariat) who identified various deficiencies and problems with the instrument. A working group was established which recommended, amongst other things, that the Model Law was no longer fit for purpose (Expert Working Group outcome statement, London, Sept 2019). These recommendations were accepted by Commonwealth Law Ministers (Sri Lanka, November 2019), with Ministers 'noting' the conclusion that the Model law no longer reflected best practice in Commonwealth countries. We continue to agree with this conclusion, and would not recommend adoption of the Model law or the structure found in the Canada Evidence Act.

Singapore

The admissibility of electronic evidence in civil and criminal proceedings in Singapore is regulated by the traditional rules of evidence. Electronic evidence is treated no differently from other forms of documentary evidence, save that s. 116A of the Singaporean Evidence Act 1893, as inserted by the Evidence (Amendment) Act 2012, provides for four presumptions that apply to the admission of 'electronic records'. The 2012 Act also repealed the original provisions governing the admission of what was previously known as 'computer output evidence', namely ss. 35 and 36 of the Singaporean Act. These provisions treated electronic evidence as a distinct category of evidence with further conditions for admissibility at trial. One avenue for admissibility was to show the evidence had been approved through an 'approved process.' Section 35(5) of the Singapore Act empowered the Minister to make regulations to prescribe an 'approved process' and appoint certifying authorities. Although the authorising provision (s. 35 of the Singaporean Act) has since been repealed, the Evidence (Computer Output) Regulations continues to apply. The Regulations allow for the Minster to prescribe an "approved process" and appoint a certifying authority, whose role remains relevant to one of the four presumptions mentioned above.

The presumptions have been considered by appellate courts in Singapore on a number of occasions. See, for example, *GIL v Public Prosecutor* [2024] SGHC 287; *Super Group Ltd v Mysore Nagaraja Kartik* [2019] 4 SLR 692; *Telemedia Pacific Group Ltd v Credit Agricole (Suisse) SA* [2015] 1 SLR 338; *Mitfam International Ltd v Motley Resources Pte Ltd* [2014] 1 SLR 1253.

We would not support adoption of the framework in s. 116A for a number of reasons, including:

1) we do not see sufficient grounds for what is presumed in the circumstances that are outlined in s. 116A.
2) The wording of the provision has rightly been described as 'rather clumsy' (*Telemedia,* [248]). There are a range of interpretative uncertainties relating to s. 116A, and aspects of its operation remain unclear. In the recent decision in *GIL,* for example, it was determined that one of the presumptions only served to facilitate admission of the evidence, but did not 'relieve parties of the burden of proving that the electronic records were reliable once they were admitted into evidence.' (*GIL,* [26]). This begs questions about the purpose of that particular presumption, and how reliability is to be separately established. These issues will likely be back before the upper courts in Singapore before long.
3) A range of questions arise as to how the presumptions interact with other provisions of the Evidence Act 1893 relating to issues such as the best evidence rule, and authentication.
4) We are concerned that there are risks of miscarriages of justice due to the operation of s. 116A, and how its interpretation and operation in the civil context translates into the criminal sphere, where there can be an obvious inequality of arms.

Australia and New Zealand

The Australian Evidence Act 1995 contain various provisions which are intended to facilitate the admission of electronic evidence. Section 146 creates a rebuttable presumption that, where a party tenders a document or 'thing' that has been produced by a process or device, if the device or process is one that, if properly used, ordinarily produces a particular outcome, then in producing the document or thing on this occasion, the device or process has produced that outcome. Section 147 provides a similar rebuttable presumption in relation to documents produced by processes, machines and other devices in the course of business.

In 2005 these provisions were considered by the Australian Law Commission, due to differences with certain State evidence laws, in particular ss 45C and 59B of the South Australia Evidence Act 1929. Section 45C dealt with the admissibility of reproductions of documents and allowed courts to determine the matter based on, *inter alia,* the certification 'of a person with knowledge and experience of the processes by which the reproduction was made.' Section 59B, on the other hand, made 'computer output' admissible, subject to the court being satisfied of a range of issues related to the functioning of the computer(s), and the reliability of its output. No equivalent provisions are found in the Evidence Act 1995, and the Law Commission considered whether a more rigorous admissibility regime for computer output, such as was found in ss. 45C and 59B

of the Evidence Act 1929, should be adopted for the 1995 Act. The Commission recommended against this,[2] having considered quite a narrow evidence base of seven submissions to their consultation.[3] Subsequently, ss 45C and 59B were repealed by ss 8 and 12 of the Evidence (Records and Documents) Amendment Act 2015. There are parallels that can be drawn here between the repeal of s. 69 PACE and the repeal of these provisions in South Australia.

See further s. 137 of the New Zealand Evidence Act 2006. Various provisions of the latter Act also deal with certification of public documents (see e.g. ss. 138 and 149).

Malaysia

The admissibility of 'document[s] produced by a computer' or 'statement[s] contained in such documents' in civil and criminal proceedings in Malaysia is governed by s. 90A of the Malaysian Evidence Act 1950 ('the Malaysian Act'. Section 90A(1) provides that in Malaysian civil/criminal proceedings, a 'document produced by a computer' or a 'statement contained in such document' shall be admissible as evidence of any fact stated therein if 'the document was produced by the computer in the course of its ordinary use' (the 'ordinary use' test), whether or not the person tendering the document/statement was its maker. The Malaysian Act does not define what amounts to 'ordinary use'. It is for the party seeking to admit the evidence to identify what amounts to 'ordinary use' on the facts. A 'document' and a 'computer' is defined in s. 3 of the Act.

In *Gnanasegaran Pararajasingam v Public Prosecutor* [1997] 4 CLJ 6, the Court of Appeal identified two methods of satisfying the 'ordinary use' test:[4]

(a) **Certification**: s. 90A(2) provides that for the purposes of proving that a document was produced by a computer in the course of its ordinary use, the party seeking to adduce the evidence may tender to the court a certificate stating the same, provided that the certificate is signed by a person who (i) either before or after the production of the document by the computer is/was responsible for (ii) the management of the operation of that computer, or (iii) the conduct of activities for which that computer was used.

(b) **Oral evidence**: alternatively, the party seeking to adduce the evidence may also call a witness to give evidence that the document was produced by a computer in the course of its ordinary use.

Where a certificate has been tendered, it is unnecessary to call the maker of the document to testify. The requirement of certification/oral evidence is not required in every case: the courts have accepted that no certificate need be produced if there is no

[2] Australian Law Reform Commission, *Uniform Evidence Law*, Report No 102 (2005), para 6.40-6.42.
[3] Ibid, para. 6.30.
[4] *Gnanasegaran* was affirmed by the Court of Appeal in *PP v Hanafi Mat Hassan* [2003] 6 CLJ 459 and partially affirmed by the Federal Court in *Ahmad Najib Aris v PP* [2009] 2 CLJ 800.

objection to the document/statement in question being tendered as an exhibit. Moreover, even in the absence of a certificate or oral testimony, the courts have taken judicial notice of certain facts to subsequently find the 'ordinary use' test satisfied.

The Malaysian Act does not set out any requirements for the form or contents of a s. 90A(2) certificate. It is sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it: s. 90A(3)(a). The certificate is *prima facie* proof of all matters stated therein, without proof of signature of the person who gave it: s. 90A(3)(b). The specific contents of the certificate will often be pivotal in whether the certificate can be successfully challenged: *Navi & Map Sdn. Bhd. v Twincie Sdn. Bhd* [2011] 7 CLJ 764.

Where a certificate is tendered under s. 90A(2), the rebuttable presumption under s. 90A(4) applies. The computer referred to in the certificate will be presumed to (i) have been in good working order and (ii) operating properly in all respects throughout the material part of the period during which the document was produced. If rebutted, this will go towards the weight of the evidence, not its admissibility.

Where a witness is called to give evidence in lieu of a s. 90A(2) certificate, the s. 90A(4) presumption does not apply.

We would not recommend adoption of the structure in s. 90A in English law for a number of reasons including:

1. There is significant risk of miscarriage of justice through the operation of the certificate system, and operation of the attendant presumptions.
2. Section 90A operates as an exception to the general rule against the admissibility of hearsay evidence. In this regard, it is also notable that (unlike the law in England and Wales) the Malaysian Act does not discriminate between real evidence (evidence created *by* the computer through information that is obtained automatically) and hearsay evidence (evidence created *by use of* the computer through human input, i.e., a Word document typed out on a computer). In other words, that which would be inadmissible hearsay as oral evidence is rendered admissible simply by virtue of it being (in) a computer-generated document. We see problems and risks with this approach.
3. There is interpretative uncertainty relating to key provisions and terms. For example, the Malaysian Act does not clarify precisely what 'good working order' or 'operating properly' means; nor does it distinguish between the operation of the physical computer (the hardware) itself versus the software used to operate the computer.
4. Section 90A's role as the sole gateway through which electronic evidence can be admitted in proceedings has been undermined in a recent series of cases relating to the common law hearsay exceptions. There is now a complex body of caselaw on this point which English law could well do without.

5. One provision relating to the accused in criminal proceedings (s. 90A(7)), carries significant risk of breaching fair trial rights and it is not clear how a provision of this nature could be justified.

India

The Indian Evidence Act 1872 governs evidence in court proceedings in India. Sections 65A and 65B were inserted by the Indian Evidence (Amendment) Act 2000 to provide for the admissibility of electronic records as evidence. These provisions provide for, inter alia, admissibility of electronic evidence by certificate from the owner of the device or its lawful operator. These provisions were considered relatively recently by the Supreme Court of India in *Arjun Panditrao Khotkar vs Kailash Kushanrao Gorantyal and Others* (2020): available at https://indiankanoon.org/doc/172105947/.

The Republic of Ireland

Section 6 of the Irish Criminal Evidence Act 1992 provides for the admissibility of documentary evidence by way of certification. For review of this provision, see the Irish Law Reform Commission Consultation Paper on "Documentary and electronic evidence"(LRC CP 57-2009) (chapter 5).

a) As examples of good practice?

We have concerns with the effect of each of the provisions that we have considered from other jurisdictions. We would not hold any out, as things stand, as examples or models of good practice.

b) As examples of things to be aware of?

The Commonwealth Secretariat's 'Guidelines on the treatment of electronic evidence in criminal proceedings' (2024) (these can also be shared upon request, pending permission from the Commonwealth Secretariat. They are yet to be published).

The 2019 Review of the Model law on Electronic Evidence.

3) If the position were to be amended, what in your opinion would be the most appropriate and practicable solution given our aims and objectives set out above? It would be helpful if your answer could address as many of the below as possible:

a) What procedural safeguards need to be in place to ensure your proposed solution is effective?

We do not think there is a straightforward solution here if the envisaged reform addresses only the common law presumption, and only with respect to certain

categories of electronic evidence. This is not likely to achieve the government's overarching objective ('to ensure fairness and justice for all those involved in prosecutions'). What is required is a comprehensive and holistic review of how the reliability of electronic evidence is addressed at the admissibility stage of the criminal trial, considering issues such as the role of presumptions, authentication, relevance and other exclusionary rules, disclosure procedures, as well as doctrines of judicial notice. For example, English law is obscure on authentication requirements for the admissibility of electronic evidence, with various divergent answers from the caselaw on whether authentication relates to relevance or reliability, and what standards of proof apply. Moreover, statutory provisions which address reliability (e.g. s. 117(7) CJA 2003 and s. 129(1) CJA 2003) are not well known in practice and their effect is unclear in fundamental respects. These issues need to be considered in the round. A review of the common law presumption(s) on its own will result in a piecemeal solution rather than the comprehensive review and reform that is required.

b) How might we ensure that any proposed solution is, as far as is reasonable possible, future-proofed?

By engaging in a more comprehensive and wide-ranging review of how the reliability of electronic evidence is dealt with at the admissibility stage of criminal proceedings. The common law presumption must not be seen as one isolated procedural 'fix'. It is certainly an area that is overdue review and reform, but as an object of study, it must be situated within its wider evidential framework of rules related to the admissibility of electronic evidence.

c) How might we ensure that any proposed solution is operationally practical?

By seeking input from trial practitioners, particularly judges. It may be necessary to embed training on any resultant reform into Law Soc and Bar trainings and to encourage the Judicial College to provide judicial training. The Royal Society might also be invited to produce a primer for the judiciary as they have done on many other topics.

d) If your proposed solution requires the use of expert witnesses (either jointly or singly instructed), what expertise and qualifications would that person require? To your knowledge are there sufficient such people at present?

N/A.

4) In your opinion, how should 'computer evidence' for these purposes be best defined?

We are not entirely clear on the 'purposes' that are being referred to here. A 'computer' is not something that has been defined previously, even in criminal statutes like the Computer Misuse Act 1990. The reason behind that decision – to avoid definition – relates to the fear that it would become technologically dated very quickly. This is

certainly a risk, and the lack of a definition has not proved problematic in the context of that particular statute. Nor is there any general legal definition of 'evidence' in the criminal law of England and Wales.

However, there are various definitions of 'electronic evidence' in international instruments, which may serve particular purposes within those documents.

For example, in the Commonwealth Secretariat's 'Guidelines on the treatment of electronic evidence in criminal proceedings' (2024) the following definitions are to be found:

> -"Electronic evidence" means any evidence derived from electronic material that may be used to prove or disprove a fact in legal proceedings.
>
> -"Electronic material" means any representation of data or information that has been stored, transmitted or otherwise processed in a computer system.

While quite general, we see value in this distinction between electronic evidence and electronic material, as this is something which is sometimes conflated in other instruments.

'Electronic evidence' is similarly defined in the Council of Europe's Guidelines on Electronic Evidence in Civil and Administrative Proceedings:

"Electronic evidence" means any evidence derived from data contained in or produced by any device, the functioning of which depends on a software program or data stored on or transmitted over a computer system or network.

In the new UN Cybercrime Convention, electronic data is defined as follows:
"'Electronic data" shall mean any representation of facts, information or concepts in a form suitable for processing in an information and communications technology system, including a program suitable to cause an information and communications technology system to perform a function.'

There is reference to 'evidence in electronic form' throughout the document, but this is not further defined.

'Electronic evidence' is defined in EU Regulation 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for Electronic Evidence in Criminal proceedings as follows:
'electronic evidence' means subscriber data, traffic data or content data stored by or on behalf of a service provider, in an electronic form, at the time of the receipt of a European Production Order Certificate (EPOC) or of a European Preservation Order Certificate (EPOC-PR);

The Council of Europe's Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence, refers to electronic

evidence in its title, but does not define it. The Council of Europe's Cybercrime Convention defines 'computer data' as follows: '"computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function.'

The UNODC Model law on Mutual Legal Assistance in Criminal Matters (as revised in 2022) defines electronic evidence as follows: 'Electronic evidence means any data or information generated, stored, transmitted or otherwise processed in electronic form that may be used to prove or disprove a fact in legal proceedings.'

a) Do you agree that evidence generated by software, as set out above, should be in scope, and that evidence which is merely captured / recorded by a device should be out of scope? Please provide a rationale for your answer.

We do not understand how this distinction would be sustainable in law or in practice. The output of software is data streams, physical displays and so on. From this, we can glean information, which may be of relevance in the criminal trial (and if so, it may become evidential material).

Data that is captured or recorded by a device will be 'generated by software.' All of the examples that were provided as 'outside' the scope of reform (digital communications, digital photographs, breathalyser readouts, mobile phone extraction reports etc) constitute computer output that is 'generated by software.' As a result, we do not see how this classification could be maintained. Nor do we see a coherent reason for excluding some of these categories. Where, for example, the metadata from digital communications is central to conviction for a criminal offence, there are obvious risks in presuming the integrity or reliability of that data, when what is presumed cannot be effectively challenged at trial and where there may be a risk of error.

Where we do see potential for maintaining some form of presumption regarding the operation of certain devices, is where the *law* has mandated the procedure for the operation of the device and in how outputs are to be generated. The courts developed presumptions to avoid it having to be proved in every instance that e.g. appointments of police officers were officially authorised with all relevant conditions having been satisfied. That approach makes sense when *the law* has prescribed a process that must be complied with before a condition is satisfied. The law is entitled to presume that its mandated process has been followed and that the standards and procedures that have been set by law were sufficient for certain legal purposes. It is, however, problematic to extend (or adopt by analogy) a similar presumption of reliability to machines: the law has not prescribed a process for their operation and functioning. Why should the law

presume regularity of a process it had no part in devising or prescribing or, in the case of complex computing systems, of which it has no understanding?

i) Can you provide specific examples of the type of evidence you believe should be in scope?

The fundamental question is whether any general presumption ought to apply as to the functioning of computers. If a general presumption cannot be coherently justified and defended, it should be abolished, with the next question then being how and whether wider rules and doctrines of evidence could be deployed so as ensure trial efficiency, where parties are not put to proof unnecessarily on matters relating to reliability within the criminal trial.

ii) Can you provide specific examples of the type of evidence you believe should be out of scope?

This depends on what is being presumed. A presumption may make more sense in certain contexts relating to, for example, breathalyser readouts, where what is presumed is limited to the accuracy of calibration, since a particular calibration may have legal consequences and will have been statutorily prescribed.

5) Are there any other factors which you believe are important for us to consider?

As above: we believe that what is required is a comprehensive and holistic review of how the reliability of electronic evidence is addressed at the admissibility stage of the criminal trial.