引文格式：庄乾龙. 加密刑事电子数据证据之关联性判断［J］. 常州大学学报（社会科学版），2021，22（6）：29-45.

加密刑事电子数据证据之关联性判断

庄乾龙

摘　要：证据的关联性具有双重含义：一是证据有能力证明案件事实，此为证据能力关联性；二是证据与案件事实之间具有实质关联性，此为证据证明力关联性。在证据能力关联性方面，加密刑事电子数据证据搜查范围与加密电子数据信息与案件信息的关联性程度相关。密码与加密电子数据信息宜并列成为刑事搜查的对象。未来立法有必要构建完善的密码提供商协助执法机构义务规则及密码搜查规则以消解加密技术导致的惩罚犯罪与保障人权之间的内在冲突。在证明力方面，加密技术将影响司法主体对加密刑事电子数据证据证明力内容的认知，并推动关联性审查判断方法的更新换代。加密技术要求在加密刑事电子数据证据证明力关联性层面以搭建虚拟与现实空间的关联性判断规则为基础，构建中间性事实与司法者背景知识的关联性判断制度。如此可有效消解法庭争议，提升司法裁判的权威。

关键词：加密；刑事电子数据证据；证据能力关联性；证明力关联性

作者简介：庄乾龙，法学博士，北京林业大学人文社会科学学院副教授。

基金项目：教育部人文社会科学研究一般项目“大数据时代刑事电子数据证据的收集与运用”（15YJC820088）。

中图分类号：DF73　**文献标志码**：A　**Doi**：10.3969/j.issn.2095-042X.2021.06.004

关联性（又称之为相关性）是证据的重要属性之一，是证据法中的核心理论，因为“一切非关联的证据不可采纳，是一个理性的证据法体系的大前提”[1]。但关联性是一个难以界定的概念，虽容易判断，但不易定性描述[2]。学术与实务层面对关联性形式与内容均有不同看法，且影响到司法适用[3]。相较于民事诉讼与行政诉讼，刑事诉讼涉及他人生命、自由及重大财产权益，在刑事电子数据证据问题上出现了立法保守而司法实践不断突破的现象。互联网双刃剑特征使得国家在重视发展运用互联网的同时，不得不关注网络安全，甚至将其上升为一种国家安全策略[4]。计算机网络加密技术在国家安全需要与商业利益驱动双重作用下获得快速发展。但加密技术使得惩罚犯罪与保障人权的传统刑事诉讼价值冲突在网络领域进一步凸显，并深刻地影响到对证据关联性的判断。

一、证据关联性的双重含义解读

（一）证据关联性学说概念纷争与评析

什么是关联性，关联性包含哪些内容，学界对此并未达成共识。有人认为，证据的关联性是指：“可以作为证据的事实，与诉讼中应当予以证明的案件事实，必须存在某种联系，即能够反

映一定的案件事实。”[5]有人称，“相关性是指作为证据的事实，必须是和刑事案件具有客观的必然的联系，对于查明刑事案件有意义的事实”[6]。有学者指出，“关联性是证据的一种客观属性，即证据事实同案件事实之间的联系是客观联系而不是办案人员的主观想象和强加的联系，它是案件事实作用于客观外界以及有关人员的主观所产生的”[7]。有人言，“所谓关联性，是指就要证事实具有得推测其存在或不存在之可能的关系。该项可以推理的事实既经特定，则可供推测资料的范围也随之而特定。如其资料不足以供推测应推理之特定之所用的，即无关联性”[8]275。有人曰，“关联性是证据的自然属性，是证据与案件事实之间客观存在的联系。在诉讼活动中，作为证据采纳标准之一的关联性必须是对案件事实具有实质性证明意义的关联性，即证据必须在逻辑上与待证事实之间具有证明关系”[9]。

我国学者对上述证据关联性概念的界定尽管有些许区别，但其共性明显，即要求证据与案件事实之间必须有客观联系，凸显客观性与联系性特征。但上述概念对客观性与联系性的重视程度不同。上述第一个、第二个概念突出关联性的客观性特征，要求证据必须与应然意义上的案件事实相关。第三个概念尽管意在强调证据的客观性，但更加突出联系性特征，且重视主观对客观事实的能动反映要素。第四个概念在弱化证据关联性之客观性特征的同时，强调司法主体根据证据推测事实是否存在的重要性。第五个概念则在突出证据的自然属性基础上，倡导证据的实质性与证明性。

在国外，对证据关联性的定义同样存有争议。在日本，“关联性是指证据对其所要求证明的事实具有的必要的最小限度的证明能力”[10]。德国立法将证据的关联性定义为实质证明力，即通过证据手段影响法官确信的能力[11]。在俄罗斯，“证据的关联性是证据的性质之一，它首先证明的是它与案件实质的联系，以及与所谓中间事实的联系，及与证明或推翻依法属于证明对象的情况而必须查明的那些事实的联系”[12]。在英美国家，具有较大影响力的定义是《美国联邦证据规则》对关联性的界定：“证据具有某种倾向，使决定某项在诉讼中待确认的事实的存在比没有该项证据时更有可能或更无可能。”[13]在学界颇具影响力的证据关联性概念是美国证据学家乔恩·R. 华尔兹教授提出的简单概念[2]，相关性是实质性和证明性的结合[14]①。与我国学者对证据关联性概念界定不同，上述域外各国更加重视关联性中的主观性要素。日本也好，德国也罢，均将证据的关联性限定为证明力，而证明的本质是相关诉讼主体说服中立裁决者的过程，证明力无非是指说服的程度而已。在俄罗斯，证据的关联性不仅仅是指证据与案件实质的联系，还突出中间事实在关联性中的重要性。中间事实的性质可能会随着证明对象、裁决主体认知不同而不同，具有较强的主观色彩。英美国家的定义更是将证据的关联性与待确认的事实连接，最终表现为更有可能或更无可能的一种倾向。

上述绝大多数证据概念将证据取证问题纳入证据能力规则范畴，将证据的相关性仅限定于对案件事实的证明程度。笔者认为，基于证据关联性本质含义考虑，上述传统概念或做法值得商榷。

（二）证据关联性双重含义解读

1. 证据关联性基本特征

在确定证据关联性概念之前，有必要厘清证据关联性几个基本特征，澄清相关概念。首先，

①证据的实质性包括以下两层意思：首先，要证事实或争议事实是实体法或程序法所规定的必须予以证明的事实。证明了争议事实的存否对定罪量刑有直接的影响。其次，证据与要证事实之间具有因果的、条件的或时空上的相关。所谓证据的证明性是指证据对要证事实具有证据支持关系，即当证据事实存在时要证事实也存在或存在更为可能；当证据事实不存在时要证事实也不存在或不存在更为可能。如果一个证据对要证事实既有实质性又有证明性，则证据与要证事实之间就具有相关性。

证据关联性专指证据与案件待证事实之间的关联性。有学者指出证据的关联性应该涵盖证据与证据之间的关联性[15]，该观点有扩大证据关联性基本含义之嫌。证据关联性与客观性、合法性同属证据的三大基本属性，上述基本属性均因案件事实而存在。质言之，离开案件事实，单个证据及证据之间并没有实际意义，证据依附于案件事实，证据缺乏独立存在的价值。这也是证据本身不能成为证明对象的根本原因。况且“如果将一般意义上的‘关联’当成‘证据的关联性’则会产生很多负面效应，使得关联性规则的理解和适用难度增大”[16]。其次，证据的关联性与客观性无关。证据的客观性主要解决证据的真实性问题，但证据与案件事实是否有关，与证据的真实性并没有必然的联系。进而言之，“某一证据是否具有相关性完全可以根据该证据本身加以判断；而某一证据是否真实则无论如何不可能通过该证据本身体现出来”[17]。最后，证据的关联性带有主观性特征。证据与案件事实是否有关联取决于司法主体根据经验、逻辑规则的判断。证据关联性的本质是证据对案件事实的证明价值，而该价值体现为以司法主体为代表的人类寄希望于依靠现有证据还原事实真相的美好愿望。此外，证明案件事实的过程也充满了主观性，法官需要“综合全案证据和全部案件事实才能加以确认，而不能模式化地、预断性地由法律或者司法解释事先加以规定”[15]。综上，证据的关联性具有双重含义：一是证据有能力证明案件事实，此为证据能力关联性；二是证据与案件事实之间具有实质关联性，此为证据证明力关联性。

2. 证据能力关联性

证据能力的概念源于西方国家。相较于我国司法实践，学术上更热衷于对这一问题的讨论。2012 年刑事诉讼法修改后，出现了若干关涉刑事证据能力的规则。有不少学者将英美法系国家的可采性规则等同于刑事证据能力规则，实则不然[18]。“证据能力的规范作用主要表现为证据的排除，而所谓证据的排除，存在两种不同的机制，其一是证据不得作为认定事实的依据；其二是证据不得在法庭调查中出现。”[19]证据能力的第一种作用机制体现为司法主体可以将所有的证据纳入法庭调查的范围，只是若其符合排除情形，则不能将其作为定案的根据。证据能力的第二种作用机制更为彻底，法官非但不能将其作为定案的根据，且不能对其进行法庭调查。英美法系国家立法设置可采性规则目的是防止不具有或缺乏证据能力的证据进入法庭影响法官心证，故其作用机制主要是通过第二种方式予以实现。大陆法系国家则更倾向于使用证据能力的第一种作用机制。通观我国刑事诉讼法对证据能力规则的适用与大陆法系国家的证据能力规则含义更为接近①。可见，承认证据能力关联性既是对现有法律体系的尊重，亦与大陆法系证据能力与证明力体系保持一致。更为重要的是，将证据关联性区分为证据能力关联性与证明力关联性可以较好地发挥两者在证明案件事实上的递进关系。诚如有学者所言：“惟证据评价之关联性，乃证据经现实调查后之作业，系检索其与现实之可能的关系，为具体的关联，属于现实的可能，而证据能力关联性，系调查与假定之要证事实具有可能的关系之证据，为调查证据之前作业，仍是抽象的关系，亦即单纯的可能，可能的可能。故证据之关联性分为证据能力关联性与证明价值关联性两种。前

①如《刑事诉讼法》第五十六条规定：“采用刑讯逼供等非法方法收集的犯罪嫌疑人、被告人供述和采用暴力、威胁等非法方法收集的证人证言、被害人陈述，应当予以排除。收集物证、书证不符合法定程序，可能严重影响司法公正的，应当予以补正或者做出合理解释；不能补正或者做出合理解释的，对该证据应当予以排除。在侦查、审查起诉、审判时发现有应当排除的证据的，应当依法予以排除，不得作为起诉意见、起诉决定和判决的依据。”这意味着上述非法证据是可以进入庭审程序的，只是不能作为定案的根据而已。而非如英美法系国家的可采性规则那样禁止上述证据进入庭审程序。此外，刑事诉讼法诸如其他全案移送制度、庭前会议形式审查制度的构建均体现了证据能力规则目的在于禁止将非法证据等作为定案的根据。

者，属于调查范围，亦即调查前之关联；后者属于判断范围，亦即调查后之关联性。”[8]276 换言之，证据能力关联性属于宏观上的、前置性的关联性，证据证明力关联性属于微观上的、核心事实的关联性。前者目标是解决证据调查的范围，后者是在确定的证据调查范围基础上，对进入调查范围的证据的证明力进行价值评判。故证据能力关联性主要关涉证据的调查程序，证据证明力关联性主要涉及证据与案件事实的内在联系。

3. 证据证明力关联性

如前所述，对证据证明力界定上有不同观点，在学说上具有代表性的一种观点是证据证明力客观事实问题，不以人们的主观意志转移而转移[20]。该观点与我国传统刑事诉讼法客观证明标准具有一致性，亦与对证据根本属性的认识有着密切的联系。1979 年颁布的《中华人民共和国刑事诉讼法》（以下简称《刑事诉讼法》）第三十一条将证据定义为“证明案件真实情况的一切事实，都是证据”，从立法上确立了“证据是事实”的立场。证据“客观说”或“事实说”也成为当时学界的共识[21]。随着对证据法学研究的深入，学术界发现“绝对的客观证据说”不具有现实性，从而提出“相对客观说”①“法律真实说”[22]等概念。1996 年刑事诉讼法修正之后，相关司法解释确认了证据的关联性；2012 年修正刑事诉讼法汲取了司法实践的成熟做法，将证据定义为可以用于证明案件事实的材料，从而在立法层面承认了证据证明的关联属性。2017 年《最高人民法院关于全面推进以审判为中心的刑事诉讼制度改革的实施意见》进一步明确证据证明力的关联性特征。该意见第二十七条规定：“勘验、检查、搜查等方式收集的物证、书证等证据，未通过辨认、鉴定等方式确定其与案件事实的关联的，不得作为定案的根据。”

证据证明力属性从绝对客观到相对客观、法律真实再到关联性的发展过程亦是主观评价因素在证据证明力中由不被承认到逐渐被承认再到被确认的过程。证据证明力关联性的本质是司法主体在诉讼活动中运用常识、经验与逻辑规则进行的一系列推定。该推定包含证据性事实、推断性事实、要素性事实与犯罪的客观要件事实。证据性事实是指控诉双方提供的证据，如控方提出的证人指出：受害人的右小腿在打斗后受伤。司法人员可以从该证据性事实中做出如下推论：受害人的右小腿确实在打斗后受伤，此为推断性事实。根据该推断性事实司法人员进一步得出要素性事实：受害人右小腿受伤是因为打斗行为造成的。在此基础上，司法人员可以得出犯罪构成要件事实：犯罪嫌疑人或被告人对受害人进行了暴力殴打行为。上述由证据性事实到要件事实的推理过程就是证据证明力相关性内涵的具体展现。从这一推理过程中，我们可以得出如下两个重要的结论：其一，证据证明力与司法主体的认识能力密切相关。换言之，证据证明力大小及有无与司法主体认识角度、逻辑推理过程有着紧密联系。不同的认识角度与逻辑推理都有可能会影响到对证据证明力的判断。其二，犯罪构成要件事实的最终得出需要其他证据的辅助，单一证据推论得出的事实并不能保证排除合理怀疑。故证据的证明力最终需要做体系化考量。因为随着证据量的增加，原先认为没有证明力的证据可能在后续诉讼中具有了证明力。反之，原先认为有证明力的证据，也可能受证据质与量的影响，在后续诉讼中失去证明力。

明晰证据关联性含义对于理解加密刑事电子数据证据关联性至关重要。因为在电子数据领域，对刑事电子数据证据关联性做证据能力关联性与证明力关联性的区分显得更为必要。下文将围绕加密技术对刑事电子数据的证据能力关联性与证明力关联性两个方面的影响展开论述。

---

①参见樊崇义：《证据法学（第五版）》，法律出版社 2012 年版，第 151 页；宋英辉、汤维建：《证据法学研究述评》，中国人民公安大学出版社 2006 年版，第 162－163 页。

二、加密技术对刑事电子数据证据关联性的影响

（一）加密技术对刑事电子数据证据能力关联性的影响

如前所述，刑事电子数据证据能力关联性与证据调查范围及调查程序密切相关。即刑事电子数据证据关联性解决的是通过何种手段获得的证据方可进入证据证明力关联性判断的视野的问题。

1. 加密刑事电子数据证据搜查范围

传统刑事搜查的对象具有空间与形态感，侦控人员只需要进入特定的物理空间就可以实现搜查的目的。但人类无法进入虚拟空间，且不能通过常规的手段搜查发现相关证据。虚拟空间证据获取与判断必须借助高科技手段。更为重要的是，加密刑事电子数据使得虚拟空间有了层次化。有学者与实务人员将其与现实空间做对比，认为可以将一般意义上的虚拟空间类比为现实空间，加密的文档属于封闭的场所或容器，对一般的虚拟空间可以进行一般意义上搜查，加密文档则受合理隐私权的保护，对其搜查需要履行特殊的搜查程序。笔者认为，这一类比并不十分妥当。首先，虚拟空间难以类比为现实空间。现实空间中的隐私权表现为人类在特定场所内相关信息、财产等的保密性。虚拟空间中的隐私权则表现为对各类数据信息的保密性。原则上，手机、电脑等能够被所有者占有控制，且他人无法直接了解的信息都属于他人的隐私。就此而言，电子数据信息的特殊存在方式使得该类信息具有隐私性特点。国外相关判例也认可电子数据的隐私性。如在Trulock v. Freeh 一案[①]中，警察凭借搜查令搜查了行为人的电脑。该判例中，将行为人电脑视为具有合理隐私期待权的对象，若对其实施搜查必须有搜查令。但当警察进一步搜查该电脑中的加密文档时，法院认为警察的行为不具有合法依据，属于违法搜查。法院的这一认定实际上将电子数据作为一般意义上的隐私对象，所有者对其数据拥有合理的隐私期待权。但上述电子数据里面的加密电子数据则成为独立的拥有隐私权的对象，警察欲对其实施搜查必须单独申请搜查令。在United States v. Runyan[②] 与 People v. Emerson[③] 案件中，法官分别将加密的磁盘与加密的文件看作封闭的容器，警察不能单凭一般意义上的搜查令就对上述加密数据信息进行搜查。因为行为人之所以对上述文件进行加密是希望上述电子数据信息不会被除拥有密码的人看到，相较于其他电子数据信息，行为人对加密信息拥有更具可期待性的隐私权，理应对其加强保护。就此而言，电子数据信息具有两层意义上的合理隐私期待权：一是非加密电子数据信息的合理隐私期待权；二是基于加密而形成的更具合理性的隐私期待权的电子数据信息。侦控机关若对电子数据信息进行搜查必须进行二次搜查令的申请，一次申请永远有效的搜查令在电子数据信息领域缺乏合理性。

需要进一步思考的是，加密电子数据信息与案件信息的关联性程度问题是否影响搜查的范围。根据加密的对象不同，电子数据加密信息范围表现出较大的差异。行为人可能会对个别的word 文档进行加密，也可能同时对包含多个文档信息的文件夹进行加密，还有可能对电脑系统中的某个磁盘进行加密，甚至是对整部电脑系统进行加密。侦查人员是否需要对所有的加密信息都进行二次搜查令的申请，这需要结合加密的信息类型进行判断。目前多数媒体设备、智能系统

①Trulock v. Freeh，275 F. 3d 391（4th Cir. 2000）.

②United States v. Runyan，275 F. 3d 499，464-65（5th Cir. 2001）.

③People v. Emerson，766 N. Y. S. 2d 482，488（N. Y. Sup. Ct. 2003）.

都带有开机密码设置。该密码一般由系统自行生成，甚至有些人不愿意使用该密码系统，但受限于系统设置只能使用。就此而言，行为人设置该密码的目的可能并非防止其他人查阅其电脑系统上的电子数据信息，而是不得已而为之。对此类因系统自带密码而成立的电子数据信息，原则上行为人不享有更具合理性的隐私期待权。侦控机关在获得一般意义上的搜查令时即拥有打开该电脑系统的权力，除非有证据证明，行为人设置该密码有其特殊的隐私期待权。这可以从以下几个方面进行综合判断：一是开机密码的复杂性程度；二是是否对开机密码系统进行了升级换代；三是打开终端设备是否就意味着对敏感信息一览无余；四是其他考虑因素。加密电子数据本身与案件的关联程度问题也是侦控机关必须予以考虑的因素。（具体如何进行判断适用，在下文中的证据能力规则部分将予以论述，在此不再赘述。）

有必要进一步探讨的是密码是否属于刑事搜查的对象。密码是打开加密刑事电子数据信息的关键。侦控机关在无法自行打开加密电子数据时，即使取得了加密刑事电子数据的搜查令，也无法实现搜集电子数据证据的目的。就此而言，密码与刑事电子数据本身是须臾不可分割的，两者没有实质性区别。司法实务中，有人认为，要求行为人提供密码与提供电子数据是不一样的，提供密码可能会受到不被强制自证其罪原则的限制，但提供电子数据本身则不会构成与这一原则的冲突[23]。这一做法只能适用于英美法系国家。因为在英美法系国家相关法律认为行为人属于广义上的证人。电子数据信息多属于系统自动生成的信息，与行为人无关，即此证据不是在侦控机关施压之下形成，故可以对其采信。但密码不同，密码可能需要行为人提供，尤其是处于动态变换中的密码更是如此。笔者认为，英美法系上述观点并不适用于我国。密码与电子数据信息具有等质性，因为侦控机关取得了电子数据的密码，就等于取得了加密电子数据信息。就此而言，刑事搜查的对象理应包括密码，受到刑事搜查规则的严格限制。换言之，侦控机关无论要求行为人提供电子数据还是密码，如果其属于对行为人自己不利的证据则理应受“不被强迫自证其罪原则”的制约。

2. 加密刑事电子数据证据获取与不被强迫自证其罪原则的关系

基于网络安全需要，网络公司与软件开发公司均在不同程度上对网络数据实施密码保护。有些软件产生的密码安全性极高，侦查机关难以破解。如腾讯公司对 QQ 聊天工具中的用户登录密码及传输密码采用不同的加密技术。一般解密软件无法破解上述密码，这给侦查机关破获案件带来较大阻力。与传统搜查不同，针对加密刑事电子数据证据的取得需要二次取证：一是搜查该加密数据的载体；二是搜查加密数据本身。传统搜查对象指向的是物理空间，侦查机关获得搜查证后，对特定物理空间进行搜查即可完成搜查任务。但侦查机关对加密电子数据的搜查与此迥异，因为侦查机关搜查到电子数据载体并非意味着掌握了电子数据证据。囿于加密刑事电子数据证据的无形性，传统针对有形证据搜查的规则难以对其适用，这甚至成为世界性疑难问题。

其实不仅仅是针对加密刑事电子数据的搜查存在疑难问题，即便是针对普通刑事电子数据证据的搜查也存在截然不同的做法。如在极为重视个人权益保障的美国，其司法实践对此也持有不同观点。一种观点认为，将加密刑事电子数据证据视为特别的隐私权，需要进行特别申请搜查。搜查的主体只能是特定的专业技术人员，在针对搜查的电子数据进行隔离的前提下，只能针对搜查令状中指定的信息进行搜查。在搜查中获取的任何多余的电子数据信息都应该及时销毁，或者返还给所有者①。另一种观点认为，只要侦查机关获得电子数据证据载体的搜查证，就意味着获

①United States v. Comprehensive Drug Testing, Inc., 621 F. 3d 1162 (9th Cir. 2010).

得了对加密电子数据证据的搜查权力，可以搜查该电子设备上的任何电子数据①。就加密刑事电子数据的搜查而言更是如此。如在某一诈骗案件中，被告人将自己的手机交给了侦查人员，但该手机加了密，侦查人员穷尽所有手段都不能将其破解。为应对这一问题，美国某些法院通常以传票的方式要求行为人提供手机密码以解锁手机。但这与其构建的任何人不被强迫自证其罪的原则可能存在冲突，美国各地法院对其持不同见解。

在 United States v. Kirschner 一案②中，被告涉嫌非法持有儿童色情照片，且将数字照片以加密文件的方式予以储存。检察官为此向法院申请传唤被告并要求被告提供密码，被告声称该做法违反任何人不被强迫自证其罪原则拒不提交文件密码。法院审查后做出了支持被告人说法的裁决，驳回检察官的传票申请。但在 In Re Boucher 一案③中，执法人员发现被告人在计算机中储存 4000 多张色情图片，执法人员怀疑上述图片中有涉及儿童的，但被告人对图片文件作了加密处理。本案中，参与调查的陪审团要求被告人提供文件密码，被告以其违背任何人不被强迫自证其罪原则为由拒绝提供文件密码。法院认为，被告人笔记本电脑中的文件内容是自己编写的，不属于证言，不受《美国宪法修正案（五）》的保护，故不支持被告人的理由，并要求被告人交出解密副本。美国法院在上述同类案件中的不同做法折射出惩罚犯罪与保障人权在加密刑事电子数据证据取舍中的冲突。上述何种做法更具有借鉴意义，我们难以做出统一判断，这必须结合我国立法与司法现实，谨慎论证加密刑事电子数据证据获取与任何人不被强迫自证其罪原则之间的关系。

新修正的《刑事诉讼法》的进步之处是在刑事诉讼基本原则部分增加了“任何人不被强迫自证其罪”原则，但遗憾的是新修正的《刑事诉讼法》依然保留了原《刑事诉讼法》第九十三条规定的“犯罪嫌疑人对侦查人员的提问应该如实回答”，该法同时规定侦查人员在讯问犯罪嫌疑人时应当告知其坦白从宽的法律规定，以至于有学者质疑“不得自证其罪”的具体适用条件[24]。大数据给传统刑事诉讼原则与制度带来的不仅仅是适用形式上的变化，还深刻地影响到内容。加密刑事电子数据更是将传统刑事取证存在的问题予以充分暴露，并集中表现为对刑事电子数据证据能力关联性影响。“就加密数据而言，对加密计算机或设备所有文件执行搜查是否构成过度搜查？当执法机构无法破解加密设备时，要求被告提供密码或解密数据是否构成自证其罪？当被告拒绝服从提供密码或解密数据的法庭命令时，应该采取何种补救机制？这些都是司法机关急需解决的问题。”[25]

（二）加密技术对刑事电子数据证据证明力关联性的影响

1. 司法主体对加密刑事电子数据证据证明力内容的认知

如前所述，对证据证明力关联性的判断离不开司法主体的一系列知识，至于该知识包括哪些内容，司法实践与学术界的知识表现出高度一致性：均通过“逻辑”“经验”“常识”等概括性术语简单带过，未有具体规定与详细论证。根据证据知识的属性不同，可以将证据知识区分为证据自身的知识与证据生成机制的知识[26]。证据自身的知识是指证据本身包含的能够证明案件的信息是什么的知识。如在犯罪嫌疑人计算机中搜查出的犯罪计划，通过该计划可以证明犯罪人的犯罪动机、犯罪过程等犯罪构成要件事实，对于该类普通证据知识，一般司法主体能准确判断其与

①United States v. Kernell, No. 308-CR-142, 2010 WL 1491873, at * 8 (E. D. Tenn. Mar. 31, 2010).

②C127 United States v. Kirschner, No. 09-MC-50872 2010 WL 1257355, at * I (E. D. Mich. Mar. 30, 2010).

③In Re Boucher. No, 2: 06-mj-91, 2009 WL 424718, at * (D. Vt. Feb. 19, 2009).

案件事实的相关性。但随着证据自身知识的变化，判断该知识是否与案件事实有关就变得困难和复杂起来。如若涉案证据为计算机源代码的侵权复制，当侦查机关查获的证据是一系列代码时，该代码与侵权代码之间关系的判断就没有那么简单了。一般而言，司法者不具备计算机源代码知识，判断其与案件事实是否相关不得不依赖于具有专业知识的人员。而专业知识的人员的判断方法是否科学，判断依据是否合理，依然需要司法主体运用相关知识予以识别。进一步而言，对于加密刑事电子数据证据相关性的判断，司法主体需要对加密这一知识进行认知，包括加密的方法、加密的安全程度、解密的方法、解密的安全程度等。若司法主体不能对上述证据自身内容进行认知，就不可能对其是否具有相关性做出准确的判断。但司法主体仅有对证据自身内容的认知还是远远不够的，司法主体还需要进一步认知该证据生成的机制。

证据生成机制的知识认知是指司法主体对犯罪行为留存证据过程应有明确的了解与把握。任何犯罪证据都是犯罪行为作用于特定对象之后留下的痕迹。在数字领域，了解犯罪行为如何与虚拟空间发生作用从而留存相关证据是司法主体在证据与案件事实之间搭建关联的重要一环。与传统现实空间发生的犯罪不同，虚拟空间的犯罪行为介入了机器设备与各种电子系统，传统的人-人互动转变为人-机-人互动关系。刑事电子数据证据带有明显的机器烙印。在加密刑事电子数据证据领域，密码生成程序、密码的设定者与密码的开启使用者是否一致都将影响到电子数据证据与案件事实关联性的认定。传统证据的关联性表现出单一性特征，刑事电子数据证据则具有明显的双重性特质。有学者称之为双联性，包括内容的关联性与载体的关联性。“内容关联性是电子证据的数据信息同案件事实之间的关联性，载体关联性是电子证据的信息载体同当事人或其他诉讼参与人之间的关联性。具体来说，前者影响案件事实存在或不存在之认定，后者确定电子证据所蕴含的信息同案件当事人等主体有无关联；前者属于一种经验上的关联性，后者属于一种法律上的关联性；前者等同于对传统证据提出的一致要求，后者体现出对电子证据关联性的特殊要求；前者主要涉及物理空间，即判断电子证据的内容是否对证明物理空间的案件事实产生了实质性影响，后者则主要涉及虚拟空间，即借助电子证据的形式确立虚拟空间的案件事实并搭建两个空间的对应关系。”[27]就加密刑事电子数据而言，司法主体必须查明对于行为人在现实空间是否实施了对特定电子数据加密的行为，并判断该加密电子数据内容与实施加密的人是否具有对应关系。

司法主体对加密刑事电子数据生成机制的认知是证据自身内容与待证案件事实建立联系的重要纽带。传统证据领域中的证据生成机制与证据自身内容之间的关系是比较隐晦的，但在刑事虚拟空间领域生成的证据将这一问题明显化，尤其是加密技术在计算机网络空间领域中的运用迫使立法者做出立法应对。

2. 司法主体对加密刑事电子数据证据关联性的审查

与客观证据观相比，证据证明关联性的本质是降低了对司法主体建立证据与案件事实之间的关联的要求。这与刑事司法领域证据证明方式的变化有着密切的关系。在现实空间，证据稀缺性特征明显，证据的“质”在认定犯罪事实中扮演着极为重要的角色，这决定了司法实践尤其重视强因果关系，重视个体证据与犯罪事实的强关联性。但在大数据背景下，海量数据证据改变了传统的证据稀缺性特征，大样本乃至全样本的证据分析变得可行。在此背景下，单个证据与案件事实的强关系转变为弱关系成为一种可能。这在一定程度上催生了关联性证据观念与制度。关联性证据制度旨在将任何带有趋向性的证据都视为与案件事实相关。换言之，“如果任何正常人在评估要素性事实（FOC）的概率时可能受到影响，那么，该证据就达到了相关性标准。这是一个鼓励采纳证据的规则”[28]。在英美法系国家，证据关联性规则设计目的在于帮助陪审团获得尽可能

多的有用信息，并限制法官的自由裁量权。而我国创建该制度的目的则更多的是迎合大数据的发展，是在海量数据、信息爆炸下，司法主体因对证据自身知识及证据生成机制知识不足而有意降低刑事司法证明门槛的应对策略。

根据加密类型不同，加密技术大致可以区分为计算机传输加密技术、信息隐藏技术、存储加密技术、确认加密技术、量子加密技术、对称加密技术、非对称加密技术、秘钥管理技术、数字签名技术等[29]。行为人对电子数据实施加密的动因无非是对外保密，不希望第三人任意翻看相关电子数据内容。加密刑事电子数据证据是相对于非加密刑事电子数据证据而言的。一般而言，前者的证明力高于后者的证明力。但我们不能将其视为适用于一切情形的统一规则。具体证明力的大小需要结合案件具体情况做出细致判断。一般而言，加密技术越高级，电子数据被篡改的可能性就越低，电子数据的真实性程度就越高，相应地电子数据证据证明案件事实的程度就越高。但电子数据证据的真实性程度不能等同于电子数据证据与案件事实之间的关联程度。对加密电子数据证据与案件事实是否相关及关联性程度高低仍需要进行个别化判断。根据加密电子数据证据形成方式不同，可以将其区分为一维加密刑事电子数据证据与多维加密刑事电子数据证据。前者是指在行为人单独与计算机系统交互作用下产生的电子数据证据，如隐藏式电子数据证据。该类电子数据证据因无法得到其他人的证实，其证明力较低。多维刑事电子数据证据是指行为人在与他人互动交流中产生的电子数据证据。该类证据因有多人的参与，其与案件事实的关系可以得到相互的验证，从而提高电子数据证据的证明力，如加密电子邮件及加密的网络论坛等。

同为加密刑事电子数据，因加密方法不同，破解难易程度各异，第三人对电子数据证据进行修改的可能性随着加密技术的复杂与安全程度的提高而降低。“如在非对称性加密技术中，RSA系统加密方法是最为复杂的一种，经过此种方法加密的电子邮件证据证明力明显大于使用其他加密技术处理后的电子邮件证据证明力，因为在这一系统加密方法中降低了私钥传输被泄露的可能。司法主体应注意对加密方法的审查，加密方法越复杂则其获得的证据证明力应越高。”[30]

三、加密刑事电子数据证据关联性法律规则的建构

（一）加密刑事电子数据证据能力关联性法律规则

1. 密码提供商协助执法机构义务规则

加密刑事电子数据证据能否进入司法者的调查范围不能一概而论，必须结合加密刑事电子数据证据类型进行分析判断。这涉及国家公共政策、商业政策等与惩罚犯罪之间的利益考量及惩罚犯罪与保障人权之间关系的协调平衡。构建有效的获取刑事电子数据证据是打击犯罪的重要手段，但加密技术很大程度上削弱了国家打击犯罪的力度。从打击犯罪的角度看，国家更倾向于对加密行为进行控制。美国于1993年发布了《密钥托管倡议》，并随后出台了《密钥托管协议》。该协议大致内容为，政府与特定部门加强对公民通信安全的保障，对公民通信实施加密措施；但当执法机构需要追查犯罪时，可以根据法庭的授权获得托管机构的密钥，从而破解相关人员的通信秘密。上述倡议与协议遭到了诸多机构与人员的反对，他们认为上述倡议、协议违反了《计算机安全法》的精神[4]，是政府对计算机安全领域的不适当干预。更为重要的是，执法部门完全有可能利用托管密钥潜在的漏洞，绕过司法机关的审查直接解密密钥，这将严重威胁到公众的通信及其他隐私安全。

我国政府对密码管理一直坚持“自主可控”的政策，对密码实行许可制度。自1999年开始，

我国先后出台了若干规范密码的文件[①]。上述文件规范的对象主要是商业密码，且未对侦查取证问题做出规定。2019 年 10 月 26 日立法机关发布的《中华人民共和国密码法》在实行核心密码与普通密码分类管理的基础上，对密码涉及的相关问题进行了较为系统的规范。但遗憾的是，作为规范密码的最高法律文件，密码法仍未对密码服务提供商就执法的协助义务问题做出清晰的规定。司法实务中，执法机构要求密码服务商提供协助的情形不在少数，而密码服务商采取了多元化的协助义务履行方式。有些案件中，密码服务提供商坚持用户利益至上的原则，拒绝将密码提供给执法机构。但在诸如贪污、贿赂等重大复杂的案件中，密码服务提供商则会配合执法机构为其提供用户的密码信息。这一度造成了司法实践的混乱局面：同一密码提供商针对不同案件采取不同的态度，不同密码提供商针对同一案件态度各异，毫无规律可循。相较于中国密码服务提供商的上述灵活做法，国外网络服务提供商在此方面表现出较大的统一性。2014 年美国苹果公司与谷歌公司升级智能手机操作系统，对用户信息进行加密，且只有用户可以进行加密。该政策的出台惊动了美国政府，相关部门紧急召开针对该行为的“加密技术”听证会，强烈反对网络服务提供商的上述加密行为。但以苹果公司为代表的中间网络服务提供商仍然以对客户做出承诺为由坚持对客户信息加密。美国执法机构无奈只能寻求其他措施以突破加密技术对侦查行为带来的障碍。

笔者认为，对加密技术采取何种政策，取决于一国对公民数据信息保护与国家安全利益的平衡。目前我国某些领域的犯罪依然十分严重，如在反腐高压下，贪污、贿赂犯罪现象虽然有所减少，但总体情况依然不乐观。随着网络技术的发展，以网络诈骗为代表的新型网络犯罪层出不穷，打击犯罪维护国家安全在较长一段时间内仍然是我国的一项重要任务。基于此，美国网络服务提供商的加密技术政策并不可取。但目前，关于密码服务提供商的执法协助义务规定过于粗疏，缺乏可操作性，亦不适合平等保护公民合法权益的法律原则精神。考虑上述因素，可以对密码服务提供商的执法协助义务做类型化的区分，明确何种情形下，网络服务提供商应该提供密码，何种情形下不具有此协助义务。具体可以通过以下两种方式进行规范或限制：一是以犯罪性质与刑罚轻重为标准进行划分。对于可能判处 10 年以上有期徒刑、无期徒刑、死刑的贪污、贿赂犯罪案件、危害国家安全的案件采用暴力手段实施的严重危及人身安全、财产权利的案件，以及网络诈骗案件，网络服务提供商有义务协助执法机构提供相关密码破解服务。二是执法机关必须有证据证明该密码涉及的内容与破获上述案件有着直接的关联性，且穷尽其他合法手段仍然无法获取被加密的电子数据文件的内容。上述两个条件应该同时具备。相应地，对于其他类型的案件，或者不符合上述条件的案件，网络服务提供商免除不具备协助执法机构的义务，且应该履行保护客户密码的义务，即应禁止网络服务提供商自愿提供密码服务行为。

2. 刑事电子数据证据中的密码搜查规则

对刑事电子数据证据的搜查涉及两个步骤：一是对电子数据载体的搜查，二是对电子数据本身的搜查。电子数据载体与传统搜查对象并无实质区别，搜查时只需要遵循传统搜查规则即可；但对电子数据如何进行搜查则是值得讨论的问题，尤其是当所搜查的电子数据被采取加密技术处理后，这一问题就变得更为突出。我国目前缺乏对加密刑事电子数据搜查的规定。在司法实务

①具体包括：《商用密码管理条例》《商用密码产品生产管理规定》《商用密码产品销售管理规定》《商用密码产品使用管理规定》《境外组织和个人在华使用密码产品管理办法》《电子签名法》《电子认证服务密码管理办法》。此外，在《国家安全法》《保守国家秘密法》《网络安全法》《反恐怖主义法》《对外贸易法》《技术进出口管理条例》中也对密码问题进行了相关规定。

中，对加密刑事电子数据的获取一般采取“一并处理”原则，即刑事搜查对加密刑事电子数据载体与电子数据本身具有同等效力。刑事搜查令状并不区分电子数据载体与电子数据本身。换言之，执法机关只要取得刑事搜查令状即可对电子数据载体与电子数据进行搜查。若刑事搜查的电子数据有密码，则既可要求犯罪嫌疑人或被告人提供，也可采取解密措施直接破解，还可要求密码网络服务提供商予以协助。总之，对上述加密刑事电子数据的处理缺乏统一、有可操作性的规定，一切是以方便获得电子数据证据为准。

域外各国做法各异，但大致分为以下几种情形：一是在区分隐私权是否合理的基础上，判断政府的电子侵入行为是否合法。在 Katz v. United States 一案[①]中，法院确立了判断加密技术信息能否成为《美国宪法修正案（四）》保护对象的主客观双重标准：主观上表现出行为人对隐私权的切实期待；客观上该期待能够为大众所普遍认可。符合这两个标准则此采取的加密信息应该依法得到保护，对其进行刑事搜查应该进行严格限制。二是第三方的例外原则。在 Miller[②] 一案中，当法院向银行送达传票后，银行将 Miller 所有银行账户信息发送给法院。法院基于银行这一第三方的自愿递交行为获得了行为人加密电子数据信息，则该刑事电子数据证据具有了证据能力关联性。三是加密文件的丢弃行为导致隐私权不受保护。在 Scott[③] 一案中，行为人将文件用碎纸机粉碎后丢弃于废纸筒，后执法机构将该碎纸拼接还原。行为人认为该文件被切碎后不能由其他人任意审阅，执法机构的行为造成对隐私权的侵犯。法院认为，行为人使用加密手段隐藏电子数据后将该电子数据丢弃并不希望执法机构破解获得数据信息的行为，不属于隐私权保护的范围。四是用提供解密副本方式代替提供密码。在英美法系国家，犯罪嫌疑人、被告人也属于证人，证人必须提交受传唤的个人信息，包括加密的电子数据信息[31]。故当行为人涉案电子数据信息被加密，法院则要求其以证人身份提交电子数据信息，以规避要求其提交密码，从而获得加密电子数据证据。五是执法机关自我研发解密软件，对加密信息进行破解。当然通过该种方式获取的加密电子数据不属于个人隐私权范畴。六是采用证人缺失推定制度[32]。该制度意指当行为人掌控着证据，且行为人不愿意交出该证据，控方又无法通过其他途径获得该证据时，法院可以指示陪审团基于上述理由推断该证据对行为人不利，从而迫使行为人交出该证据。

我国司法实践与国外相比灵活性有余，可操作性不足。国外相关规则相对丰富，但其做法也并非尽善尽美。以美国为代表的西方法治发达国家，一般将加密数据信息作为个人隐私予以对待，从而对其予以合法保护，若对其进行搜查则必须严格遵守相关法律规定；当搜查加密刑事电子数据侵犯个人隐私权时，则执法机关获得的电子数据信息应当予以排除。在上述 Miller 一案中，银行作为独立第三方披露了行为人的加密电子数据信息，法院将银行的这一做法作为第三方例外予以采纳有一定的法理根据。但通过此种方法获得加密数据，独立第三方是否履行了银行保密义务是值得推敲的。倘若允许或鼓励该行为，则极有可能会诱发执法机关通过额外的力量动员独立第三方“自愿”交出行为人的加密刑事电子数据信息。如此，保护商业秘密与打击犯罪之间的就很难达致平衡。法院以要求行为人以证人的身份提供解密副本代替要求其提供密码，这是在英美法系国家特有的广义证人制度下方行得通的方法，对我国并没有太大的借鉴意义。相比较而言，证人推定缺失制度有着更强的借鉴意义，可以考虑以此为基础构建中国特色的加密刑事电子

①Katz v. United States, 389, U. S. 347, 361 (1967).

②United States v. Miller, 425, U. S. 435, 443 (1976).

③United States v. Scott, 95 F. 2d 927 (lst Cir. 1992).

数据证据搜查制度。

一切合法的电子数据信息原则上都应受到法律的保护，尤其是加密电子数据信息。但当电子数据信息属于违法犯罪信息时，侦控机关拥有对其控制的权限。但当电子数据信息被加密时，我们无法通过被加过密的文件或者载体判断该数据信息属于合法信息还是违法信息，只有破解密码后方可了解该电子数据信息的性质。尽管我国刑事搜查制度并没有明确该制度保护的对象，但根据搜查的范围与内容，我们也能大致得出该制度保护的对象包括住宅安宁权、隐私权及个人信息数据权等。这也是刑事搜查为什么需要以取得搜查令为前提的原因。当公民加密电子数据信息时，其目的是不想让第三人知晓该电子数据信息内容，故公民原则上拥有对加密电子数据信息的隐私权或数据信息权。执法机关若要取得该电子数据信息则必须获得搜查令。一旦执法机关通过搜查令合法获取了电子数据加密信息，则权利人就丧失了对该加密信息的控制，执法机关拥有对该加密电子数据信息进行破解的权利。在此情形下，执法机关可以通过开发解密软件的方式破解该加密电子数据。但当执法机关无力破解该加密数据信息时，则需要通过其他合法途径获得该加密电子数据信息的密码。为此，可以考虑设计如下途径：其一，合法获得第三人的帮助。该第三人主要涉及三类群体，第一类是附加义务的密码提供商。若案件属于上文提到的特殊案件，密码提供商有义务协助执法机关破解该密码。第二类是掌握该密码的其他证人。如共同掌握密码的第三人，若其愿意向执法机关提供所掌握的密码，则执法机关可以用此密码破解加密刑事电子数据信息。第三类是未附加义务的密码提供商。若本案属于上述特殊案件，密码提供商自愿打破商业秘密规则，向执法机关提供密码的，执法机关视为合法获得密码，有权以此密码破解加密刑事电子数据信息。其二，构建同意搜查制度。尽管司法实践中已然承认同意搜查，但规则阙如。未来立法有必要进一步完善同意搜查规则，使其形成制度化体系。在此制度下，若行为人自愿交付密码，则执法机关可以就此合法获得该密码并予以破解。其三，为贯彻我国刑事诉讼法确立的任何人不被强迫自证其罪的原则，借鉴吸收国外的证人缺失推定制度。该制度是指当有证据证明只有行为人掌握着该证据时，且该证据可能是唯一的，对证明案件事实将起到关键性作用时，法官可以推定该证据对行为人不利，以此迫使行为人提出该证据。在加密刑事电子数据证据中，就转化为迫使行为人交出密码[33]。如此，可以打破行为人的证据优势，实现控辩平等。

当然，因电子数据信息的无形性，确定哪些电子数据信息与案件有关并不是一件容易的事情。原则上，执法机关在申请搜查令状时，应就搜查的文件类型、存储路径等内容予以明确，执法机关只能在令状范围内进行搜查。司法实践中，因行为人加密对象不同，搜查范围可能会有差异。如行为人若对整部计算机进行了加密，则执法机关必须分清哪些文件与案件有关，将无关的文件过滤掉。但若有关文件信息与无关文件信息混杂在一起，需要一并搜查时，执法机关不能将无关的文件信息予以泄露或者非法使用。若行为人只对与犯罪有关的电子数据信息进行了加密，则执法机关只能针对该加密电子数据信息进行搜查，对其他无关的电子数据信息不能进行搜查；若无关的电子数据信息能够与加密刑事电子数据信息分清，则执法机关原则上应将无关的电子数据交还给行为人。若执法机关在搜查中没有遵守上述规定，给行为人造成损失的，执法机关应负担赔偿义务。此外，立法应该赋予行为人合法的救济途径，以使行为人能够保护自己受损的合法权益得到及时的补救。

（二）加密刑事电子数据证据证明力关联性法律规则

加密刑事电子数据证据证明力关联性本质上属于事实、经验判断范畴，与法律没有关系，属于自由裁量范畴。对其设置其他诉讼程序、制度相似的细致规则等缺乏可行性。但在司法实践

中，因缺乏关联性法律规则的指引，司法者对其讳莫如深，要么回避这一问题，要么武断地认定关联性的有无或者大小。尤其是司法者对涉案当事人的关联性认定质疑不予以回应，会降低司法裁判的可接受性，削弱司法权威。

1. 虚拟与现实空间的关联性法律规则

如前所述，电子数据证据与物理空间内的证据证明力有明显差异。物理空间内的证据证明力具有直接性，即某一证据与案件事实可以直接发生关联从而证明案件事实。虚拟空间的电子数据证据需要进行二次关联，方可对案件事实起到证明作用。证据均由载体与信息组成[34]，物理空间的证据只需要关注其信息或内容即可评价其证明力；但电子数据证据载体可以影响信息的证明力。判断电子数据信息内容与案件事实之间是否有关联性或关联性之大小的前提是证据载体具有关联性。从形式上看，载体的关联性主要涉及不同空间领域转换关系的确认，即需要将虚拟空间留存的证据信息与现实空间的行为主体进行对应。对于加密刑事电子数据而言，需要证明行为人在虚拟空间留存的证据信息是该人所为。

就此而言，加密刑事电子数据中的虚拟与现实空间的关联性主要包括以下几个方面：加密身份的关联、加密行为的关联、加密载体的关联与加密时空的关联。加密身份的关联是指对刑事电子数据进行加密的人的身份与案件行为人有关联。如在一起网络诈骗案件中，被告人否认向被害人发送过加密短信。从被害人提供的加密短信中无从得知发送短信的人是谁，则被告人很可能会被作无罪处理。加密行为的关联是指行为人实施了加密电子数据的发送或储存等行为。如在某一谋杀案件中，有一封谋杀恐吓的加密电子邮件被发送给被害人。行为人承认该加密电子邮件是自己制作的，但其否认实施过发送行为。其辩称可能是诸如黑客等人侵入其计算机系统冒充行为人实施了发送行为。本案中查明发送该加密邮件的人的身份对于该案件的查明有着重要的作用。加密载体的关联性是指承载电子数据信息的载体与案件当事人的关系。如某网络诈骗案中，执法机关获得一部加密手机，经解密得知行为人正是通过该部手机实施了多次诈骗行为。执法机关在讯问犯罪嫌疑人时，该犯罪嫌疑人否认该加密手机是自己的。又如在 2016 年发生的“快播公司涉嫌传播淫秽物品牟利罪一案”中，辩方质疑控方提出的服务器硬盘少了一块，从而否认该服务器硬盘来自快播公司，从而否定控方的指控[35]。加密时空的关联性具体又可以细分为时间的关联性与空间的关联性。时间的关联性是指行为人在虚拟空间内实施的犯罪行为与现实空间的时间具有联系。如行为人通过发送加密文件使计算机感染病毒的计算机显示时间与现实空间中用户计算机感染病毒的时间不一致，则难以认定行为人的行为与案件事实之间存在关联。空间的关联性是指行为人实施加密电子数据的行为发生的虚拟空间 IP、MAC 地址是否为行为人所使用。如行为人通过加密手段对他人的股票进行交易练手，造成他人股票重大损失，其行为涉嫌故意毁坏财物罪，侦查机关对其立案侦查。行为人辩解称，尽管该行为是通过自己电脑 IP 地址进入目标系统，但也极有可能是他人非法使用了自己的 IP 地址进行登录。就该案而言，若行为人的辩解成立，则其犯罪行为就不能成立。

就目前来看，立法层面尚缺乏有针对性的关联性审查规则。司法实践中，司法机关对上述当事人的抗辩多采取回避的态度。个别司法判例虽然对其抗辩进行了回应，但缺乏说服力。基于上述分析，笔者认为，结合加密刑事电子数据的特征，虚拟与现实空间的关联性规则的构建应基于当事人的抗辩进行设置。

首先看加密身份的关联性规则。在执法机关收集到无身份证明的加密电子数据后，司法主体宜从以下两个方面进行审查判断主体身份：一是加密的数据类型，根据加密数据类型进行主体身

份的推断，若属于特殊加密类型，行为人的专业属性是重要筛查对象；二是结合 IP 地址、系统登录时间、视频资料及相关证人证言等证据进行综合审查判断行为人的身份。在有特定涉嫌犯罪行为人，但该行为人否认自己是加密电子数据发送者、制作者时，可以从其是否实施过同类型的特殊加密方法对数据信息进行加密的行为进行审查判断。若有证据证明，行为人所采取的加密方法极为特殊，且在其相关电子数据文件中发现有该类型的加密电子数据类型，则可推定行为人具有实施该行为的嫌疑，但行为人能够提出反驳证据的除外。行为人采取的是一般加密类型的刑事电子数据则不宜以上述方法进行推定，而需要结合其他综合性证据进行进一步审查判断。

其次是加密行为关联性规则。在该类型的关联性判断中，行为人身份确定，只是行为人否认实施过特定行为。当行为人否认其实施过诸如发送加密电子邮件等特定行为时，司法主体应着重审查行为人对该电子数据行为的控制能力。若行为人对该数据行为能够绝对控制，则可认定行为人实施了该行为。如发送的加密电子数据信息只有针对特定对象方可起到作用，在他人无法破解该加密电子数据信息的情况下，可推定行为人对该加密数据信息进行了推送行为，除非行为人能够提出有效的抗辩证据。若行为人对该数据行为只能进行相对控制，则其加密身份是否具有关联性则需要结合案件中的其他证据进行综合判断。

再次是加密载体的关联性。在此类关联性指控中，行为人的抗辩理由表现出较大的一致性：侦控机关提出的加密数据信息设备并非为行为人所有或者单独所有。对此，司法主体应着力于以下几个方面的审查：一是加密电子数据设备的型号、品牌、颜色及外观等；二是加密电子数据设备上留存的指纹、使用记录；三是加密电子设备中其他行为人的关联性电子数据信息。上述方法应综合采用。司法实务中，不乏办案机关只是简单地以上述第一种审查对象作为推断行为人拥有电子设备的证据，这是不够的。因为同类型、品牌乃至颜色的设备并非单一的，不能排除其所有者为他人。

最后是加密时空的关联性，具体区分为加密时间关联性与加密空间关联性。加密时间关联性是指加密刑事电子数据证据的形成时间应与物理空间内的时间保持一致。司法者对此需要重点审查加密刑事电子数据证据中系统时间与物理时间本身是否一致。绝大多数虚拟空间实施犯罪行为的时间与物理空间发生的时间是一致的，但可能由于主客观原因，有时系统时间与物理时间并不一致。司法主体在审查时应关注执法机关在搜集该证据时，原系统时间与物理时间是否一致，如果不一致，其时间差值是多少。这对后续认定作案时间极为重要[①]。加密空间关联性审查的重点应该是虚拟地址是否为行为人所有，该地址是否存在他人共有的情形。根据行为人抗辩的通常理由——被他人冒用，司法者应着力审查他人冒用的动机、冒用的可能性群体等因素。同时，需要结合该地址被使用的时间，行为人当时所处的物理空间证明等因素进行综合判断加密刑事电子数据信息与行为人之间的关联性。

2. 证据与案件事实的关联性法律规则

证据与案件事实的关联性又称为电子数据信息或内容与案件事实之间的关联性。在确定证据

①在一起伪基站犯罪案件中，为了查证嫌疑人利用伪基站发送短信的行为造成多少用户通信中断，警方聘请专家对嫌疑人电脑中的发送记录和日志进行了检验。但是，在送检之前警方提取电脑时，发现“电脑系统时间与北京时间不吻合”，即电脑系统时间不反映物理空间时间，而由于疏忽也未能记录电脑系统时间与物理时间的实际差值。这就造成了对中断通信用户数的鉴定意见缺少时间关联性的困扰。参见冯潇洒：《国外加密与执法案例分析及其对我国密码立法的启示》，《信息安全研究》2018 年第 4 期 ，第 201—210 页。

与案件事实的关联性法律规则之前，应该了解司法者将证据与案件事实进行关联的过程。证据本身无所谓立场，其本质是中间性的，故证据性事实又可以称之为中间性事实。证据证明力的关联性的关键问题也就在于司法者如何看待这一中间性事实。以下以具体个案说明这一关联过程。假设证人乙向执法机构证明甲在该地区发生恐怖袭击之前的10分钟内将一封加密的电子邮件发送给了一个神秘的阿拉伯人。包括司法者在内的所有人在看到乙的证言之后都可能认为甲发送的该电子邮件可能与恐怖信息有关。当我们看到乙的这份证言之后就会把我们自己的专业知识、生活经验等与上述中间性事实关联起来。就本证据而言，司法者在看到“恐怖袭击”一词之后就会敏感地联想到该事实也许与恐怖袭击事件有关。“10分钟”说明时间比较短，而“加密”一词更能让我们有理由怀疑该电子邮件内容有不可告人之处。也许有人认为“神秘”一词是证人的意见不能作为证据来使用，但“意见”与“事实”本来就难以区分，况且乙完全可能有其他证据能够证明此人的“神秘”之处，或者行踪表现比较诡秘，或者打扮比较可疑，等等。就此而言，司法者不会轻易将这一不确定的“意见”排除掉。结合其他关键词的理解，司法者更有可能会接受“神秘”这一词语。“阿拉伯人”作为中东特殊地区的人员本身值得警惕。综合上述因素，司法者就可能推断该加密电子邮件可能涉嫌犯罪。就此而言，证据证明力的相关性本质是让一个司法者相信这一中间性事实或主张，从而为司法者在对某事实难以确定时进行确信的推断。

由此，我们可以得出一个简单的结论，证据证明力的相关性实际上是证据事实与司法者背景知识的关联性。可以肯定的是，在法庭上呈现的证据无法自发证明案件事实。该证据与案件事实发生关联需要在多方主体的努力下方能实现。其中一方是对证据的解说者或者使用者，司法实践中主要是控辩双方。上述主体需要努力将该证据性事实或中间性事实嵌入司法者的先前专业知识、逻辑经验中去，让司法者接受该中间性事实，从而为后续事实的判断做准备。如此，该证据就是相关的。反之，若该证据性事实并没有被司法者的经验、知识所接受，则该证据即使在客观上与案件事实有关，也不可能成为影响案件事实的证据。但需要引起注意的是，即使在某一单个证据性事实没有使司法者产生倾向性认识的情况下，司法者一般也不会断然以该证据不具有相关性而将其予以排除。这在国外称之为附条件的相关性。在我国，法官通过对证据的综合审查判断实现上述目的，可以说是殊途同归。就上述案例而言，司法者可能认为该电子邮件内容与行为人涉嫌恐怖犯罪有关，但若后续解密该电子邮件内容后发现其内容与犯罪事实无关，则该电子邮件就不具有关联性。可见，证据证明力的相关性在案件中不是固定不变的，而是动态的，与相关人员的诉讼主张密切相关，亦与证据的量及司法者对证据的综合评价紧密关联。

加密刑事电子数据证据证明力相关性的特别之处是中间性事实的特殊性。加密技术具有专业性、复杂性及多变性特征，一般而言，司法者凭借既有的专业知识与逻辑经验难以应付疑难复杂的采用加密技术形成的刑事电子数据证据。如加密之后的计算机病毒能否感染特定的电子信息文件，就是极为专业的问题。此时，司法者不得不依赖专业技术人员，而专业人员使用加密技术有时会依赖于人工智能。将人工智能运用于刑事司法的目的是“将统一的证据标准镶嵌到数据化的程序中，减少司法任意性，推进以审判为中心的刑事诉讼制度改革的目标”。但从人工智能运用于刑事证据判断的发展趋势来看，除了证据指引、单一证据的校验之外，司法机关还在努力尝试使人工智能具有判断证明标准的功能[36]。人工智能是逻辑性的，但司法证明过程则充满了非逻辑性，是逻辑与非逻辑的统一，是经验与逻辑的统一，人工智能难以实现证明任务。就此而言，司法者绝不能完全依赖于专业人员。换言之，应将专业人员的作用限制于解释说明加密技术的原理，可能存在的技术风险，而该风险导致的法律风险必须由司法者进行判断。就此而言，专业人

员的角色相当于帮助控辩双方就专业性的证据性事实或中间性事实向司法者做出说明，从而使司法者产生倾向性认识。进一步而言，庭审中的专业人员需要做控辩区分，且法庭一般不宜作为聘请专业人员的主体。专业人员作为控辩双方中的人员可以努力起到向司法者解释证明的作用，若由法庭自己聘请专业人员解读加密技术原理，则可能会产生不公正的误导。

综上，加密刑事电子数据证据与案件事实关联性审查判断应注意以下情形：首先，加密技术的专业人员解读不能代替司法者的裁判，原则上该专业人员应由控辩双方聘请。其次，司法主体对加密刑事电子数据证据证明力的判断是一个动态的过程，贯穿于整个刑事审判活动中，既表现为对单个证据的审查，又应体现为对总体证据与案件事实关联性的考察。在证据证明力判断上不宜设置中间性的排除规则，只能做终局性的总体考察之后方能确定何者具有证明力，能够作为定案的依据。最后，司法者基于专业知识、经验对证据性事实进行推断从而得出构建要件事实结论只要符合逻辑推论过程，符合其既有经验知识，即使出现案件认定错误，也不宜认定为错案。因为司法者的知识与经验难保完全正确。尤其是随着互联网的发展，加密技术的日益复杂化，司法者不能及时储备日新月异的知识是正常现象，因为该原因而导致的倾向性认识产生误差，从而做出不准确的事实推定，并非由于司法者的主观过错造成。

参考文献：

[1] 沈达明. 英美证据法 [M]. 北京：中信出版社，1996：130.

[2] 乔·R. 华尔兹. 刑事证据大全 [M]. 何家弘，译. 北京：中国人民公安大学出版社，1993：64.

[3] 汤维建，卢正敏. 证据“关联性”的涵义及其判断 [J]. 法律适用，2005 (5)：24-26.

[4] 冯潇洒. 国外加密与执法案例分析及其对我国密码立法的启示 [J]. 信息安全研究，2018，4 (3)：201-210.

[5] 陈一云. 证据法学 [M]. 北京：中国人民大学出版社，1991：101.

[6] 程荣斌. 中国刑事诉讼法教程 [M]. 北京：中国人民大学出版社，1993：169.

[7] 陈卫东. 刑事诉讼法学 [M]. 北京：中国人民大学出版社，2004：153.

[8] 陈朴生. 刑事证据法 [M]. 台北：三民书局，1979.

[9] 何家弘. 从应然到实然：证据法学探究 [M]. 北京：中国法制出版社，2008：33-34.

[10] 我妻荣. 新法律学辞典 [M]. 董璠舆，译. 北京：中国政法大学出版社，1991：249.

[11] 罗森贝克，施瓦布，戈特瓦尔德. 德国民事诉讼法 [M]. 李大雪，译. 北京：中国法制出版社，2007：819.

[12] 古岑科. 俄罗斯刑事诉讼教程 [M]. 黄道秀，王志华，崔煜，等译. 北京：中国人民公安大学出版社，2007：214.

[13] 美国联邦刑事诉讼规则和证据规则 [M]. 卞建林，译. 北京：中国政法大学出版社，1996：105.

[14] 张继成. 认定证据相关性的逻辑性标准 [J]. 证据学论坛，2001，3 (2)：417-431.

[15] 陈卫东. 论刑事证据法的基本原则 [J]. 中外法学，2004，16 (4)：411-440.

[16] 奚玮，刘晓东，余茂玉. 证据关联性问题之研究：以证明力为考察视角 [EB/OL]. (2006-10-29) [2021-05-30]. http://www.law-lib.com/lw/lw_view.asp?no=7728.

[17] 马秀娟. 论证据的关联性及其判断 [J]. 政法学刊，2008，25 (6)：19-23.

[18] 申君贵. 关于诉讼证据能力之探讨 [J]. 政法论坛，1993 (6)：70-80.

[19] 纵博. 我国刑事证据能力之理论归纳及思考 [J]. 法学家，2015 (3)：72-85.

[20] 陈伶俐. 证据相关性的判断与规则构建 [J]. 法律适用 (司法案例)，2017 (24)：66-71.

[21] 阳平. 从客观性到相关性：中国证据法学四十年回顾与展望 [J]. 浙江工商大学学报，2018 (6)：118-130.

[22] 樊崇义. 客观真实管见：兼论刑事诉讼证明标准 [J]. 中国法学，2000 (1)：114-120.

[23] REITINGER P R. Compelled production of plaintext and keys [J]. University of Chicago legal forum，1996 (1)：195-197.

[24] 梁欣. 不得自证其罪原则适用的几个问题：兼评刑事诉讼法修正案 (草案) 第 49 条 [J]. 法律适用，2012 (3)：30-33.

[25] 熊志海，周国平. 美国加密数据的强制性披露 [J]. 时代法学，2013，11 (1)：106-111.

[26] 周洪波. 证明标准视野中的证据相关性：以刑事诉讼为中心的比较分析 [J]. 法律科学 (西北政法学院学报)，2006 (2)：

83-94.
[27] 刘品新. 电子证据的关联性 [J]. 法学研究，2016，38 (6)：175-190.
[28] 罗纳德·J. 艾伦，张保生，强卉. 证据的相关性和可采性 [J]. 证据科学，2010，18 (3)：365-382.
[29] 方芳. 加密技术对计算机网络的影响与应用 [J]. 网络安全与技术应用，2017 (4)：58-59.
[30] 庄乾龙. 论加密技术对电子邮件证据力的影响 [J]. 时代法学，2012，10 (2)：37-43.
[31] 吴宏耀. 反对强迫自证其罪特权原则的引入与制度构建 [J]. 法学，2008 (6)：20-27.
[32] LARKIN J E D. Compelled production of encrypted data [J]. Vanderbilt journal of entertainment & technology law，2012 (1)：253-258.
[33] STIER R H J. Revisiting the missing witness inference-quieting the loud voice from the empty chair [J]. Maryland law review，1985 (44)：137，175-176.
[34] 陈瑞华. 刑事证据法学 [M]. 北京：北京大学出版社，2012：63.
[35] 快播涉黄案公开庭审全程文字实录[EB/OL]. (2016-01-08) [2021-03-09]. https：//tech. qq. com/a/20160108/062986. htm.
[36] 赵艳红. 人工智能在刑事证明标准判断中的运用问题探讨 [J]. 上海交通大学学报（哲学社会科学版），2019，27 (1)：54-62.

Relevance Judgment of Encrypted Criminal Electronic Data Evidence

Zhuang Qianlong

Abstract：The relevance of evidence has dual meanings：one is that the evidence has the ability to prove the facts of the case，which is the relevance of evidence capacity；the other is that there is a substantial relevance between the evidence and the facts of the case，which is the relevance of the probative force. In terms of the relevance of evidence capacity，the search scope of encrypted criminal electronic data evidence is related to the degree of relevance between encrypted electronic data information and case information. Passwords and encrypted electronic data information should be juxtaposed to be the subject of criminal searches. In the future，it is necessary for legislation to construct a comprehensive password provider to assist law enforcement agencies in obligatory rules and password search rules，which will alleviate conflicts between the punishment of crimes and the protection of human rights caused by encryption technology. In terms of the probative force，encrypted technology will affect the judicial body's perception on the content of probative force of encrypted criminal electronic data and will promote the update of the relevance review method. Encrypted technology requires that in the level of the relevance of the probative force of encrypted criminal electronic data evidence，it is necessary to base on the construction of the relevance judgment rules of the virtual and realistic space so as to construct the relevance judgment system of intermediate facts and judicial persons' background knowledge，which can resolve court disputes effectively and enhance the authority of judicial adjudication.

Keywords：encryption；criminal electronic data evidence；relevance of evidence capability；relevance of probative force

（收稿日期：2021-07-02；责任编辑：晏小敏）