在司法实践中，非法获取私人数字货币案件时有发生，对于该行为的罪名认定主要存在盗窃罪和非法获取计算机信息系统数据罪的争议。定性争议源于实务中对行为对象的梳理不全面、法益界定存在分歧以及行为评价不统一，其行为对象包括密码或私钥、计算机系统以及私人数字货币，分别对应数据法益、计算机信息系统安全以及财产法益。在具体定性中，非法获取私人数字货币可以分为侵害数据法益类与非侵害数据法益类。对于侵害数据法益类型，结合行为侵害的其他法益，分别认定为非法获取计算机信息系统数据罪与盗窃罪构成牵连犯、以及以上两罪的牵连犯与非法控制计算机信息系统罪数罪并罚。对于非侵害数据法益类型，可分别认定为盗窃罪以及盗窃罪与非法控制计算机信息系统罪数罪并罚。

罪名 关键词	盗窃罪	非法获取计算机信息系统数据罪

表1

在剔除盗窃电力和盗窃“挖矿”设备等与本文研究对象不相符的样本后，定性为盗窃罪的案件共5件，定性为非法获取计算机信息系统数据罪的案件共14件。实践中还存在敲诈勒索、诈骗等非法获取数字货币的案件，但这类案件对于明晰盗窃罪和非法获取计算机信息系统数据罪在非法获取私人数字货币案件上的适用并无帮助，所以不在本文的研究范围内。

（二）非法获取私人数字货币案件的适用困境

我国禁止私人数字货币融资但不禁止私人持有和交易的态度、相关立法具有较大的解释空间以及非法获取私人数字货币的理论研究不够深入等原因，造成实践中非法获取私人数字货币案件出现以下困境。

1.行为对象的梳理不全面

笔者通过对19件案例进行梳理，发现以上案件的行为模式可以概括为“打破控制+转移占有”，“打破控制”主要包括获取密码和控制计算机系统两种方式，“转移占有”则是指将私人数字货币转移到自己账户或提现等操作。实务审判中缺

乏对所有行为对象的梳理评价，以盗窃罪定罪的案件易忽视“打破控制”的行为对象即“密码或私钥”和“计算机系统”；以非法获取计算机信息系统数据罪定罪的案件则仅关注“计算机系统”，而忽视“密码或私钥”和“私人数字货币”。此类案件的审判往往陷入先入为主、以预判主导论证之中。

2.法益界定存在分歧

与行为对象的梳理不全面“一脉相承”的是，对于该行为侵害法益的梳理亦存在缺漏。以盗窃罪定罪的判决中只论及“财产法益”，而以非法获取计算机信息系统数据罪定罪的判决往往只提及“计算机系统安全”。

除了以上缺漏外，实践中对于私人数字货币表征的法益界定亦存在争议。我国央行等五部委于2013年12月发布的《关于防范比特币风险的通知》（以下简称《通知》），将比特币定义为“一种特定的虚拟商品”，但是该《通知》实质是“以一个模糊的概念来界定另一个模糊的概念”。实务判决中存在几种观点：一是“比特币是一种特殊的互联网商品，具有现金价值，属于他人的合法财产”；二是“阿希币是虚拟货币，其法律属性是计算机信息系统数据，存在相应价值，但与金钱财物等有形财产、电力燃气等无形财产存在明显差别”；三是“虚拟货币是虚拟商品，但它不是实物，且缺乏稳定性，没有现实的效用性，不能认定为刑法意义上的财物，其实质是动态数据组合，可视为计算机信息系统数据”。综上，实务中对私人数字货币表征的法益存在“财产法益说”“财产法益否定说”以及“数据法益说”。

3.犯罪行为的评价不统一

我国刑法第287条规定：“利用计算机实施金融诈骗、盗窃、贪污、挪用公款、窃取国家秘密或者其他犯罪的，依照本法有关规定定罪处罚。”最高人民法院研究室《关于利用计算机窃取他人游戏币非法销售获利如何定性问题的研究意见》则建议：“采用技术手段非法获取包括虚拟财产在内的计算机信息系统数据的行为，应当以非法获取计算机信息系统数据罪论处。”可见，我国立法与司法研究意见对于利用计算机技术盗取虚拟财产案件的处理意见相左。以上立法规定和司法研究意见必然影响法院对犯罪行为的评价，不少判决将其作为法律依据或者是论证理由引用，从而导致行为人的犯罪行为高度相似，而判决结果大相径庭的情况。例如，“黄方骏盗窃案”和“田华凤非法获取计算机信息系统数据案”，两行为人均是在帮助他人投资比特币的过程中，采用非技术手段获知了被害人比特币钱包的账号和密码，并利用其将被害人比特币转移。判决结果则是黄方骏构成盗窃罪，田华凤构成非法获取计算机信息系统数据罪。“武宏恩盗窃案”和“冯国仕非法获取计算机信息系统数据案”，两行为人通过QQ远程操作获取了被害人存放于计算机的投资平台的账号和密码，后将被害人比特币转移或变卖。法院

判决武宏恩成立盗窃罪，冯国仕成立非法获取计算机信息系统数据罪。又如“胡志凯盗窃案”和“许武浩非法获取计算机信息系统数据案”，两行为人通过非法获取的邮箱数据库，登录被害人邮箱，利用“密码找回”修改了与邮箱相关联的被害人投资平台密码，并登录平台账户进行比特币变卖或转移。法院判决胡志凯构成盗窃罪，许武浩构成非法获取计算机信息系统数据罪。

二、非法获取私人数字货币行为对象的厘清

获取私人数字货币作为非法获取私人数字货币案件的最终目的，在多数法院的判决中成为了唯一的评价对象。以持有的主体为标准，私人数字货币可以分为交易平台拥有和个人持有。对于交易平台持有的数字货币，侵入交易平台网站是主要的行为模式；对于个人持有的数字货币，其模式可概括为以各种手段获得密码或私钥后获取数字货币。故此类案件的行为对象除私人数字货币外，还应当包括交易平台网站即计算机信息系统、数字货币钱包私钥和交易平台密码。

（一）私人数字货币

实践中关于私人数字货币是什么的问题存在误解，法院判决中多采取“将电子钱包中的数字货币转移”的表述，认为虚拟货币是存储在数字货币钱包中的数据。

1.私人数字货币的概念

私人数字货币是与法定数字货币相对的概念，根据数字货币的发行机关不同，可以将数字货币分为两大类，法定数字货币是由中国人民银行发行的法定货币的数字化形式，私人数字货币是由私人发行并运用区块链技术发行、管理、流通的货币，包括比特币、以太坊等虚拟货币。数字货币的概念并不统一，基于认识和使用习惯的分歧，数字货币也被称为加密货币或虚拟货币。

数字货币诞生于现代密码学，以区块链技术作为底层支撑技术。数字货币不需要借助第三方开户，用户通过在计算机终端上安装数字货币钱包，即可开设账户。在安装过程中，本地会根据电脑特有的参数信息随机生成私钥，后本地通过特定算法导出公钥，经过两次哈希运算并整合得到一个长位数，即钱包地址。钱包地址全网公开，相当于商业银行的账号，私钥则相当于密码。在没有中介的情况下，钱包与钱包之间可以直接开展交易。区块链上的每个节点都可以将发生的交易记录下来，并通过工作量证明机制决定最终的记账人。需要注意的是，数字货币钱包具有钱包之名而不具有钱包之实，虽然可以显示该账户的数字货币存量，但是该存量是对记录在区块链同一地址的所有数字货币交易进行结算后得出的数值，其存储的是数字货币的私钥，而非数字货币本身。

2.私人数字货币的特征

中国人民银行等五部委将数字货币定义为虚拟商品。该定义并非是从刑法层面对数字货币做出的界定，但是表明与传统商品相比，私人数字货币具有以下特征：无体性和交换价值的有限性。

（1）无体性

通过上文对私人数字货币技术原理的梳理可知，数字钱包存储的是私钥，区块链上分布的是交易记录，私人数字货币既不存储在数字钱包之中，也非分布于区块链之上，乃是对区块链上同一地址的所有交易进行结算后得出的数值。私人数字货币不具有实体，是一个纯粹的概念。正如前文所述，法院对于私人数字货币的法律属性认识存在分歧，部分判决将私人数字货币定性为计算机信息系统数据。即使相关司法解释将非法获取计算机信息系统数据罪中的“数据”限缩为“支付结算、证券交易、期货交易等网络金融服务的身份认证信息”以及“其他身份认证信息”，即使目前“数据”的范围正处于扩张趋势，也无法囊括私人数字货币。因为一般的数据不论是存储于电脑还是存储于云端服务器，至少具备数据的本体，而私人数字货币不具有数据实体，公钥、私钥以及区块链上的记录都不是数字货币本身。

（2）交换价值的有限性

马克思在《资本论》中提出资本社会中所有的商品都具有使用价值和交换价值两个维度。所谓商品的使用价值是指能够满足人们一定的需要，典型商品的使用价值包括服务和劳动力的使用价值。交换价值是指商品的交换能力，其表现形式是价格或是商品在售卖时能够得到的东西或货币量。私人数字货币是一种作为概念存在的虚拟物，其本身并未凝结无差别的人类劳动，不具有传统意义上的商品使用价值。但在信仰数字货币的社群内范围内，可以实现其购买商品的能力，亦可进行数字货币之间以及数字货币与法定货币的兑换，但不像法定货币以国家信用背书，私人数字货币具备的是一种有限的交换价值。

（二）计算机信息系统

根据我国刑法以及相关司法解释的规定，“计算机信息系统”和“计算机系统”是指具备自动处理数据功能的系统，包括计算机、网络设备、通信设备、自动化控制设备等。由于交易平台密码和数字钱包私钥多存储于计算机系统中，因此一般情况下，行为人在获取交易平台密码或数字货币钱包私钥时可能会侵入被害人的计算机系统；对于直接登录交易网站的行为当然会将计算机系统作为行为对象。实践中只有以非法获取计算机信息系统数据罪定罪的判决会主动将计算机信息

系统作为行为对象评价，以盗窃罪定罪的判决则直接略过这一行为对象。

（三）数字货币钱包私钥和交易平台密码

私人数字货币在我国主要发挥投资功能，私人数字货币的持有者买进和卖出私人数字货币的交易分为两种：一种是去中心化交易平台上交易，即数字钱包之间的直接交易，这种交易方式中私钥是转账和接收并使用的关键。私钥是数字货币所有权的象征，本质是一串由字母和数字随机组成的64位字符，可以从互联网上将热钱包或冷钱包下载到自己的计算机、移动电话或其他数字设备，用于储存私钥。私钥的泄露和损毁意味着持有者的数字货币资产暴露于随时被侵犯的危险之中或者其数字货币资产永远无法找回。

另一种是中心化交易平台上的现货交易，类似于股票市场的交易。由于去中心化交易不能挂单买卖，成交花费时间长，故我国大部分的数字货币交易是通过中心化交易所进行的。中心化交易平台的交易原理可以概括为：通过注册成为平台用户，交易所会为每一名用户分配一个钱包地址。从事交易的第一步是向交易所充值，平台用户将法定货币支付给平台，平台从自身持有的数字货币总量中转移相应数额至用户的钱包地址；或者用户通过自己其他钱包向平台分配的钱包地址充值，交易所则会显示用户的账户内有对应的数字货币。交易所用户账户的数字货币会定期归集到交易所的主钱包地址中，因此用户从平台分配的钱包地址向其他钱包提币实际是从交易所主钱包地址的转移。需要注意的是平台内交易通过登录平台账号和密码即可进行操作，因此平台内交易并不引发区块链的交易记录，仅表现为用户交易平台账户的数字货币数值的增减。对于钱包之间的直接交易，则需要转账方知道对方的钱包地址和公钥，并用自己的私钥对转账报文进行签名并全网广播，引发区块链的交易记录。

三、非法获取私人数字货币侵犯法益之界定

通过上文梳理可知，非法获取私人数字货币的行为对象包括私人数字货币、计算机信息系统、钱包私钥和交易平台密码。私人数字货币所承载的法益应界定为财产性利益，计算机信息系统表征的则是计算机信息系统安全，钱包私钥和交易平台密码本质属于数据。

（一）私人数字货币的法益论证

关于私人数字货币的属性，存在货币说、数据说、物权客体说以及债权说。由于2013年央行等五部委出台的《通知》明确表明比特币不是真正意义上的货币，另外比特币作为一个纯粹的概念，并不具有“数据”实体，所以对于数字货币的争议应当限缩于物权客体和债权之间。无论是物权客体说还是债权说都是对私人数

字货币具有财产属性的肯定，这两派观点来源于民法上对私人数字货币的界分，延伸到刑法领域则分别对应财产犯罪中的财物说和财产性利益说。

1.物权客体说

有学者认为，虽然比特币不属于物理意义上的有体物，并非传统民法意义上的物，但是用户可以通过私钥排他性地控制与支配数字货币，基于管理可能性说，数字货币可以成为物权的客体。持反对意见的学者认为，根据物权法定原则，数字货币没有被规定为物权法上的“物”，所以数字货币不能成为物权客体。基于此观点，有学者提出反对意见，即判断虚拟财产（该学者认为虚拟货币是一种虚拟财产）是否是物的实质不在于物权法的规定，而应当根据其是否具有物权客体的属性进行判断。虚拟财产满足可由特定的时、空加以固定的一种现实客观存在的特定性和可按照一般社会观念得以完整存在的独立性，可以成为物权的客体。但是正如前文所述，数字货币不具有实体甚至不具有数据本体，其不满足“现实客观存在”的要求，并且数字货币只具有交换价值不具有内在的使用价值，脱离了其运行的区块链网络，数字货币无法独立完整存在。因此根据该学者主张的实质判断标准，数字货币亦无法成为物权的客体。

阻碍数字货币被评价为物权客体的因素有二，即物权法定原则和数字货币的非客观存在性，这是当前持“物权客体说”的学者无法解决的问题。

2.债权说

有学者参考日本法院的判决，“绝大多数案由是合同、无因管理与不当得利等债权法律关系纠纷”，根据我国民法典第118条第2款规定“债权是因合同、侵权行为、无因管理、不当得利以及法律的其他规定，权利人请求特定义务人为或者不为一定行为的权利。”从而建议将数字货币当事人的权利定性为债权。另有学者从虚拟货币的实质进行分析，认为虚拟货币的权利内容实际上是“当事人可将他人承认之持有单位数向其他参加者移转之权利，且该持有单位数须经他人承认才有正当性。”据此应当属于债权。持债权否定说的学者理由则较为统一，即数字货币的去中心化导致发行人和债务人缺位，故不存在对特定人的债权。

笔者赞同“债权说”，在数字货币开发者编写的程序中可以解读出相关的权利与义务，如数字货币程序管理者的资格、程序治理规则、程序变更规则等。以比特币为例，其程序规则大致可以概括为原始取得数字货币的规则与继受取得数字货币的规则。原始取得即数字货币采取分布式共享账本，区块链上的每个节点都有一个账本，每个节点都能检测、验证账本信息，通过数学题决定最终的记账人，获得记账权的人可以得到系统自动奖励的一定数目的比特币。继受取得则是预先知道对方的钱包地址和公钥后，转账方用自己的私钥对转账报文进行签名并全网

广播。全网收到该转账信息后进行验证，最终持有钱包地址私钥的人才能够使用这笔资金。区块链上的每个节点在加入区块链时可视为已经默示接受以上规则，每一个节点的负责人既是权利人又是义务人，例如请求其他节点对转账信息进行验证的权利和验证转账信息的义务，这种权利和义务通过程序的设计而自动行使和履行，与传统债权行使方式不同。值得一提的是，以中心化交易所为平台进行数字货币的交易，主要是指交易所的内部交易，通过向交易所发出指令，经交易所审核后，在平台内发生数字货币的转移或者兑换，在这一场合，数字货币则体现为用户对交易所的债权。

与德国、日本刑法明确区分财物与财产性利益不同，我国刑法侵财犯罪中未出现“财产性利益”，仅有“财物”一个概念，但我国刑法通说承认财产犯罪中的“财物”是包含财产性利益的广义概念。张明楷教授提出不论是财产性利益还是狭义的财物，只要具备三个特征即可作为财产犯罪的对象，第一，具有管理可能性，数字货币的管理可能性可以通过钱包私钥、交易平台密码或者交易平台网站管理权限实现；第二，具有转移可能性，数字货币虽不具有实体，但可以在钱包或交易平台账户之间进行转移，并表现为区块链上或平台上相应的交易记录；第三，具有价值性，凡具有一定交换价值或一定使用价值，原则上就是财产犯罪的行为对象。数字货币的单一价值性不妨碍其成为财产犯罪的行为对象。有学者则持反对观点，认为虚拟财产不能归入“财物”，只能以侵犯著作权罪进行补充保护。知识产权的客体首先应当是人类的智力成果，私人数字货币是由“矿工”们依赖于各自“矿机”的计算能力，争夺记账权而产生的，其本身并不具有任何智力创造。因此即使学界对数字货币的属性仍存在物权客体说和“债权说”的争议，也不影响数字货币成为财产犯罪的行为对象。

（二）数据法益作为新兴法益的证成

当前我国司法实践对“数据”的理解较为混乱，一方面，相关司法解释将“数据”限定为“包括账号、口令、密码、数字证书等在内用于确认用户在计算机信息系统上操作权限的身份认证信息。”；另一方面，从实践判决来看，“数据”几乎涵盖了所有可以在计算机系统中储存、显示、获取的权利客体。不论采用何种理解，交易平台密码和私钥均可被囊括进“数据”的范畴之内。而私人数字货币由于不具有数据本体，则自然无法采取数据法益保护路径。“由于我国数据犯罪在体系上隶属于刑法第285条和第286条所规定的计算机犯罪，保护法益也受制于计算机信息系统安全”，导致对数据法益的保护不足。下文将论证数据法益是具有独立性的新兴法益。

1.对数据法益进行独立保护的必要性

“所有的法益都是生活利益，而生活利益是社会生活实践产生的。”新兴法益的

产生是社会生活实践发展的必然产物，刑法并不保护所有的生活利益。在判断刑法的保护法益时，必须遵循一定的规则。首先，应根据宪法的基本原理确定哪些生活利益可能成为刑法上的法益；其次还需要考虑利益的价值、法益陷入危险的频率以及危险的程度等因素。最后，还应当考虑数据法益独立的必要性。

（1）数据法益具有保护价值

罗克辛教授提出，法益概念显然是以宪法的描述为基础，产生于国家的根本任务。首先，需要在宪法中寻求法益的价值基础。根据是否经过技术加工，可将数据分为结构化数据和非结构化数据即元数据，未经过技术加工的数据即元数据，社会公众是其主要提供者，以个人信息为内容，具有人身属性。结构化数据则是在元数据的基础上经过加工所得，无论是结构化数据还是非结构化数据都间接或直接与我国宪法保护的公民私有财产和公民隐私等基本权利紧密相关。

国务院2015年印发《促进大数据发展行动纲要》，指出“数据已成为国家基础性战略资源”。2016年11月7日颁布的网络安全法，将保障网络数据的完整性、保密性、可用性的能力界定为网络安全的一部分。中国工业和信息化部电信研究院（现称中国信息通信研究院）于2014年、2016年、2018年、2019年、2020年及2021年度陆续发布大数据白皮书，根据党中央、国务院的重要指示，提出了“将数据资源转化为经济发展动力的课题”，“推动实施国家大数据战略，加快建设数据强国”，“数据成为继土地、劳动力、资本、技术之后第五种市场化配置的关键生产要素”。2019年8月30日，我国发布《信息技术安全—数据安全能力成熟度模型》，规定了数据采集、数据传输、数据存储、数据处理、数据交换以及数据销毁六个阶段的数据安全要求。2021年6月为规范数据处理活动，保障数据安全，促进数据开发利用，保护个人、组织的合法权益，维护国家主权，颁布数据安全法。可见，对于数据的发展与保护早已提上国家战略层面，数据法益无疑具有保护的必要性。

（2）数据法益危险频发

纵观计算机犯罪的发展史，早期作为数据载体的计算机信息系统是犯罪的主要攻击对象，近年来，数据承载了更重要的价值，成为了主要的攻击对象。2019年2月，我国人脸识别公司深网视界曝出数据泄露事件，超过680万条身份证信息、人脸识别图像及GPS位置记录等被泄露。不仅如此，侵犯数据安全犯罪已经呈现出产业链模式，我国“网络黑产”从业人员已超过150万，市场规模已高达千亿级别。尽管当前我国对数据的地位与性质尚存争议，但通过刑法来保护数据安全已然成为了我国立法与司法的选择。

（3）计算机信息系统安全笼罩下的数据法益欠缺全面保护

我国数据犯罪栖身于刑法第285条第2款非法获取计算机信息系统数据罪和第286条破坏计算机信息系统罪第二款的计算机犯罪之中，对“数据”的定义亦借助了“计算机信息系统”这一概念，即“计算机信息系统中存储、处理或者传输的数据”。与计算机信息系统的概念存在相互定义的问题。传统观念认为数据存在于计算机系统之中，侵犯数据必然会侵犯计算机系统。例如，有观点认为破坏计算机信息系统罪第2款的成立必须满足在破坏数据的同时，还必须影响计算机信息系统功能的正常运行。此种保护模式并不直接保护数据本身，而是将数据安全作为计算机信息系统功能运行的一部分进行保护，此种间接的保护方式意味着不影响计算机系统运行的数据安全无法得到相应保障。随着数字化技术的发展，数据与计算机信息系统之间的“承载与被承载”关系变得松弛，侵害数据安全的行为不一定必然同时侵害计算机信息系统安全。我国数据法益在立法和司法上受制于“计算机信息系统安全”，导致数据法益定位模糊，数据犯罪与传统犯罪界分困难，无法应对日新月异的数字化犯罪技术。因此数据法益应当跳脱“计算机信息系统安全”的笼罩，独立成为一项新兴法益。

2.数据法益作为新型法益的可行性

根据是否经过技术加工，可将数据分为结构化数据和非结构化数据即元数据。

元数据表征的是数据的保密性、完整性和可用性，其内容是一系列权利集合。首先，基于元数据的内容与数据主体的人身、财产等密切相关，衍生出下列权利：第一，知情同意权，即未经数据主体的知情同意，相关数据应当处于保密状态，包括数据收集者在内的其他所有人不得获悉、收集、利用相关数据；第二，被遗忘权，即数据主体将其信息上传网络后，应当具有无理由删除的权利，其他义务主体应当配合。其次，出于对电子数据这一媒介的信赖，产生以下权利：第一，维护数据完整性的权利，这一项强调的是数据相对方应承担维护数据完整性的义务，应当保证数据不被删除、修改或增加等；第二，使用权，是指数据相对方应当确保数据主体能够及时、有效地访问和使用存储于电子媒介的个人数据。

结构化数据是用户为获得经济利益或某种社会评价、服务时主动提供或者专门的数据经营者通过用户协议收集的元数据，经过数据经营者的收集、整理和分析等处理后具有了实用性，能够为权利人带来经济利益的数据。其蕴含的是公平自由的数据市场秩序。数据经营者的加工使得元数据之上附着了数据经营者的劳动和智慧，应当受到法律保护。但若直接以数据产品权利人的权益作为保护客体，可能会导致没有实际侵害权利人利益但已经严重妨碍数据市场公平自由竞争的行为无法入罪。例如，“酷米客诉车来了盗取后台数据案”中，元光公司法定代表人授权技术人员利用爬虫技术大量获取竞争对手“酷米客”软件中的实时公交信息，以提高旗下同类软件的市场用户量和信息查询准确度。元光公司的恶意爬取行为并未造成“酷米客”的直接损失，但是却已经破坏了公平自由的市场秩序。“

十四五规划纲要”对未来大数据发展作出总体部署，其中提到“发展数据要素市场，加强数据产业制度建设”，以及数据安全法第19条提出“培育数据交易市场”。作为数据产品利用、交易的主要场所，数据市场具有重要的战略地位，公平自由的数据市场秩序应当成为刑法的保护对象。另外，将公平自由的数据市场秩序定性为“结构化数据”表征的法益，不意味着数据产品权利人的权益不受保护，相反数据产品权利人的合法权益正是此种秩序能够作为刑法保护客体的价值基础，这种秩序并非仅关注某个具体权利人的权益，而是为了社会公众的公平自由的市场秩序普遍不受损害。

3.数据法益作为新型法益的挑战性

数据法益作为独立于计算机信息系统安全的新兴法益，计算机信息系统安全应当从数据犯罪中脱离。而数据法益与计算机信息系统安全法益分离后，该如何对二者分别提供刑法保护，则是数据法益作为独立法益将面临的挑战。

《欧盟网络犯罪公约》将计算机系统与计算机数据分别作为独立的侵犯对象，以不同的罪名予以规制。非法访问与系统干扰侵害的是计算机系统安全，其保护法益表现为计算机系统的不被侵入与系统功能的正常运行。我国刑法中有相关罪名与之对应，非法侵入计算机信息系统罪的保护法益是特定计算机信息系统的不被侵入的保密性；破坏计算机信息系统罪第1、3款以“造成计算机信息系统不能正常运行、影响计算机系统正常运行”为构成要件，保护的是计算机系统正常运行的有用性；非法控制计算机信息系统罪保护的则是计算机信息系统不被控制的保密性，成立该罪不要求造成计算机系统不能正常运行。

侵犯数据主体的知情同意权、被遗忘权，属于违背数据主体的意愿，阻止数据维持或恢复保密状态，应当以刑法第285条第2款非法获取计算机信息系统数据罪定罪处罚。但对于数据主体主观上对数据不具有保密的意思，并且客观上亦无采取相应保密措施的数据的获取，不属于违背数据主体的意愿。侵犯数据主体维护数据完整性的权利或使用权，是一种破坏数据的行为，不仅包括物理意义上的破坏即删除、修改和增加，还包括对数据使用可能性的破坏，应当以刑法第286条第2款的规定定罪处罚。在数据法益的指导下，成立该罪不要求对造成计算机信息系统不能正常运行，这并非数据法益涵盖的范畴。

综上所述，对于计算机信息系统安全的保护应当集中于非法侵入计算机信息系统罪、非法控制计算机信息系统罪以及破坏计算机信息系统罪第1、3款。非法获取计算机信息系统数据罪和破坏计算机信息系统罪第2款则成为纯粹的数据犯罪另外还需要对以上两个罪名进行相应的修改完善，因元数据与结构化数据表征的法益分别是个人法益和秩序法益，故建议在以上两罪名中以侵犯对象为标准设置两款具体规定。

四、非法获取私人数字货币行为的分类及定性

一般而言，非法获取私人数字货币的行为分为两个阶段，第一个阶段是打破权利人对私人数字货币的控制，第二个阶段则是获取私人数字货币，属于共性环节。案件差异体现在第一阶段，或是获取密码或私钥，或是直接进入交易所网站。根据第一阶段侵犯的法益不同，笔者将案件划分为侵害数据法益类和非侵害数据法益类。

（一）侵害数据法益类

钱包私钥与平台密码是非法获取私人数字货币案件中的主要工具，其表征的是数据法益。

序号	行为类型
类型三	a.通过日常行为获取平台密码或私钥，再利用平台密码或私钥窃取数字货币（案例三） b.利用网站管理权限合法登录交易所网站，进行窃取数字货币的操作（案例四）

表3 非侵害数据法益的行为类型

1.类型三：单纯侵害财产法益

（案例三）被害人常某邀请被告人冯国仕通过QQ远程帮其操作“阿希币”钱包参与空投项目，常某将“阿希币”钱包私钥存放在电脑桌面，远程操作期间被告人冯国仕多次打开此钱包并复制钱包私钥。后被告人冯国仕利用私钥将其价值约21万元的“阿希币”盗走。法院判决被告人成立非法获取计算机信息系统数据罪。

日常行为与“侵入计算机信息系统”和“其他技术手段”的区别不在于手段方式是否借助计算机技术，而在于被害人对于其平台密码和钱包私钥是否采取保密措施。被害人邀请被告人帮助投资数字货币，在此过程中被害人必然会接触到钱包私钥，主观上被害人对钱包私钥将暴露于被告人无疑是明知且同意的，在客观上钱包私钥不再处于完全保密的状态，至少被害人未对被告人采取保密措施。因此，即使被告人采取了“其他技术手段”，但因为被告人获取钱包私钥的行为并不侵犯被害人数据法益中的知情同意权，故这一行为应当被评价为合法行为，并未侵害数据法益。

（案例四）自2015年起，被告人仲崇杰担任比特币大陆公司运营维护开发工程师，2017年被告人通过使用“TEAMVIEWER”软件远程控制其在比特币大陆公司工位上的电脑，使用ROOT权限进入公司的服务器，转移100个比特币至个人钱

包中，造成公司损失人民币36000元。法院认定被告人构成非法获取计算机信息系统数据罪。

被告人仲崇杰的网站管理权限是由被害人比特币公司赋予的，这意味着该网站内的程序或存储的数据等在一定程度均是对被告人公开的，被告人的登录并不侵犯公司网站的保密性，被害人的计算机信息系统安全并未受到负面影响。

2.类型四：侵害计算机信息系统安全和财产法益

（案例五）被告人周翔担任区融未来公司客服一职，与被告人李陟预谋侵入公司计算机信息系统，获取虚拟货币。被告人周翔利用工作中获取的公司同事的账号登入公司BI网后台管理系统，获取虚拟货币约355万个，违法所得100余万元。法院认为被告人行为构成非法获取计算机信息系统数据罪。

案例四与案例五均是利用网站管理权限进入交易所网站，不同的是案例五中被告人周翔本身不具备登录资格，意味着交易所网站对被告人采取了保密措施。即使利用他人权限非暴力登录网站后台，但未经被害人许可的登录也是对网站后台保密性的侵犯。

（案例六）被告人魏成峰与朱某预谋通过黑客技术入侵数字货币交易网站后台数据库，朱某通过该网站后台存在的漏洞使用“菜刀”黑客软件入侵网站后台，并通过技术手段将网站后台比特币转出至魏成峰账户，违法所得额为475000元人民币。法院判决被告人成立非法获取计算机信息系统数据罪。

被告人利用黑客技术侵入网站后台的行为会对被害人网站后台的保密性甚至可用性造成损害，这类案件必然侵犯计算机信息系统安全。

（三）非法获取私人数字货币的类型化定性

笔者将私人数字货币定性为债权类财产性利益，若非法获取私人数字货币的数额达到盗窃罪的入罪门槛，那么第二阶段必然成立盗窃罪。

1.类型一：非法获取计算机信息系统数据罪与盗窃罪择一重罪论处

获取私人数字货币的犯罪途径有两种，对于个人持有的私人数字货币，获取的方式限于先获取平台密码或私钥再获取数字货币。平台密码或私钥本身就是一串字符，唯一的用途即是控制私人数字货币，获取平台密码或私钥的目的往往是进一步获取数字货币，所以，获取平台密码或私钥与获取数字货币之间是手段与目的的牵连关系。

类型一借助其他技术手段获取平台密码或私钥的行为侵犯被害人关于个人数据的知情同意权，应当成立非法获取计算机信息系统数据罪，第二阶段的行为成立盗窃罪。两行为之间存在牵连关系，按照牵连犯的处理规则，应当择一重罪论处。

2.类型二：牵连犯择一重处后与非法控制计算机信息系统罪数罪并罚

类型二在类型一的基础上增加了“侵入被害人计算机信息系统”这一行为，侵害了计算机信息系统安全，应当成立非法控制计算机信息系统罪。若实践中侵入被害人计算机系统已经造成系统无法正常运行，则应当适用破坏计算机信息系统罪第1或3款。因此，类型二需要在非法获取计算机信息系统数据罪与盗窃罪成立牵连犯，择一重罪论处的情形下与非法控制计算机信息系统罪或破坏计算机信息系统罪数罪并罚。

3.类型三：单独成立盗窃罪

类型三应当单独成立盗窃罪。被告人获取私钥或者登录网站后台是经被害人知情同意的，行为并未侵犯数据法益或者计算机信息系统安全法益，第一阶段的行为属于合法行为，只需对第二阶段做出评价即可。

4.类型四：非法控制计算机信息系统罪与盗窃罪数罪并罚

不论是利用管理权限的非法登录还是非利用管理权限进入网站，均是未经同意的非法行为，侵犯交易所计算机系统的保密性甚至是系统的有用性，因此，应当成立非法控制计算机信息系统罪或适用破坏计算机信息系统罪，并与盗窃罪实行数罪并罚。