破坏计算机信息系统罪罪量要素的界定

于改之[1],宋　灿[2]

(1. 上海交通大学凯原法学院,上海　200030)
(2. 华东政法大学刑事法学院,上海　200042)

摘要:实践中破坏计算机信息系统罪的行为方式具有类型化特点,实务裁判时有成为他罪"兜底罪名"的倾向。为解决实践中的适用泛化问题,需确定本罪罪量要素的体系定位,厘清罪量要素所限定的法益内涵,重新界定罪量要素的具体内容。体系上,罪量要素属于典型的构成要件要素,要求行为人认识到其所依托的基本事实及对事实的规范性评价,但后者只需达到社会一般人评价的严重程度即可。内容上,罪量要素要求行为侵害法益"系统正常运行"后还需满足"量"的要求才可成立本罪。为限制本罪的适用,应排除与体系定位不符的"违法可得"标准,将"社会影响"外延限定在本罪的不法量域内,严格解释"直接经济损失"标准,同时"举重以明轻",适度扩张适用侵害结果持续时间的"时长"标准。

关键词:破坏计算机信息系统罪;罪量要素;系统的正常运行;构成要件要素
中图分类号:D914　　**文献标识码**:A　　**文章编号**:1673-1565(2023)05-0041-12

随着网络的普及和发展,计算机等自动化处理数据系统已然突破了固有印象中物理设备的桎梏,渗入社会生活,成为必不可少的生产要素。[1]虚拟世界构建了新的社会现实,构成平行现实的复本。数字化的社会进程带来了刑法研究的视域转变,近年来学界更多将焦点放至"数据"这一微观存在,忽视了对中观形态——"系统"的研究。但事实上,随着端的联网泛化与重要系统的集中化,破坏计算机信息系统的行为一方面严重损害公民的安全感,易造成具身性的集体恐惧;另一方面也严重威胁国家安全。破坏计算机信息系统的特定技术不断出现,在现实中已经能够脱离以技术知识为纽带的人身依附关系,主体即使不具备特定技术知识也可实施破坏行为,相关科技风险迭代频发,呼唤刑事层面的回应。《中华人民共和国刑法》(以下简称《刑法》)第 286 条规定了破坏计算机信息系统罪,规制妨碍系统运行的行为。但自由与安全如法之两翼、车之两轮,保护安全亦不可忽视自由流动的重要性。为充分实现数据要素价值,激活数据要素潜能,不应忽视对系统安全的关注,应在"安全—自由"的价值间寻找恰当的落脚点,立足实践现状,实现数据自由流动与系统稳固安全的利益平衡,为数据经济提供助推,为数据发展提供保障。

一、实务样本分析与问题的提出

为使本罪规治与当下互联网的发展相契合,首先需明确本罪的实践适用情况。笔者在"北大法宝"网站以"判定罪名:破坏计算机信息系统罪""审结日期:2019. 01. 01 至 2023. 10. 16""案件类型:刑事一审"为检索条件,共获 2019 至 2023 年间案例 271 份。通过研判 271 份判决文书,笔者发现破坏计算机信息系统罪在实践中存在行为上的"类型化"趋势与适用上的"口袋化"倾向两个特点。

(一)本罪行为方式具有类型化特点

实务案例大多集中于几种行为样态,笔者将其总结如下。第一类,删除、修改、增加系统"规

收稿日期:2023-09-10
作者简介:于改之(1969-),女,山东聊城人,上海交通大学凯原法学院教授,博士生导师,主要研究方向为刑法学。
宋灿(1999-),女,山东枣庄人,华东政法大学刑事法学院刑法学硕士研究生,主要研究方向为刑法学。

则数据”①妨碍系统运行的行为。实务中存在技术职业人员为发泄、报复等目的,删除公司系统规则数据的判例。② 第二类,删除、修改、增加系统“内容数据”但未妨碍系统正常运行的行为。案例中常表现为在交通系统内删除违章数据,在志愿填报系统内修改学生信息等。这类行为在实践中常与“滥用权限”“收受好处”等附随情状行为具有牵连关系,但实务中一般仅以破坏计算机信息系统罪评价。③ 第三类,利用系统规则等“作弊”手段致使系统运行效率降低或无法正常运行的行为。这种状况下系统仍然依循“规则数据”设定的规则运行,但系统本身不可用。常见类型为 DDoS 一类占用系统合理资源的行为,④如利用苹果手机遗失查找功能锁定手机的行为。后者常与诱骗当事人登出手机 ID,待系统无法正常运行后向当事人索要“解锁费”等诈骗或敲诈勒索行为牵连出现。索财等非法占有目的是此类行为的重要动因。⑤ 第四类,通过修改、增加、删除内容数据导致系统输出结果“失真”的行为。Fiddler 抓包行为是典型的行为样态,其原理是采用“中间人攻击”的方法,即在客户端与服务器之中插入 MITM(Man-in-the-MiddleAttack),通过 MITM 与真实的客户端及服务器形成链接,抓取、解密、修改在二者间传输的报文数据。⑥ 第五类,改变外部物理环境致使系统输出结果“失真”的行为,实践案例多与污染环境类犯罪相关,利用棉花堵住滤网,擅自更换检测样本等是常见的行为手段。⑦

(二)本罪实践适用具有泛化倾向

笔者认为实践中的“适用泛化”问题主要体现在以下几个方面。

首先,不当扩展本罪危害结果的含义。《刑法》286 条第 1 款规定了违反国家规定,对计算机信息系统功能进行删除、修改、增加、干扰造成计算机信息系统不能正常运行且后果严重的行为。其中,“造成计算机信息系统无法正常运行”这一结果与破坏行为之间具有刑法上的因果关系,且被立法明文确定,故学界通说将其视为本罪构成要件中的危害结果要件。[2] 从短语的通常文义出发,“系统无法正常运行”是“系统功能”角度下对危害结果的描述,与系统输出结果的“真伪”并无关联。但实务中却常常将“系统是否运行”理解为“系统输出结果是否真实”,以结果的“真实性”替换系统功能运转的“可能性”,将没有妨碍系统运行的行为也认定为本罪。以最高人民法院发布的 104 号指导案例⑧为例,法院认为李某某、张某某用棉纱堵住滤网造成监测数据失真干扰了计算机信息系统功能,造成了系统不能正常运行的后

① 本文所称的“规则数据”是与“内容数据”相对的所指。“规则数据”是规定系统如何运行的数据,即设定系统运行规则的数据;“内容数据”则是不涉系统运行规则的、依循“规则”运行的数据。以“2+3=5”这一算式为例,“+”为确定系统运算逻辑的“规则数据”(决定本算式的计算规则是加法运算),“2”“3”为依循系统计算逻辑的“内容数据”(依照计算规则执行加法运算并得出相应结果)。

② 被告人吴某入职上海蕴某信息科技有限公司(以下简称蕴某公司)先后全职、兼职承但公司产品的技术开发、运营和管理等工作。后被告人吴某因双方发生劳动争议离职,遂产生删除公司数据讨要薪资的念头。2020 年 10 月,被告人吴某利用蕴某公司文件服务器存在的漏洞,使用 rm 指令删除了蕴某公司服务器中的相关数据,导致蕴某公司开发的 APP 无法实现图形闭合功能。参见上海市长宁区人民法院(2021)沪 0105 刑初 382 号刑事判决书。

③ 如贺某某为获取高额报酬,诱使考生填报“预报名系统”,非法获取数十名考生的信息,通过猜密码的方式登入考生志愿填报系统,擅自将考生志愿修改为与其存在利益往来的学院或职业学校后将志愿锁定。共有 11 名考生因贺某某篡改志愿行为被错误录取。参见广西壮族自治区南宁市青秀区人民法院(2019)桂 0103 刑初 188 号刑事判决书。

④ DDoS 攻击全称为分布式拒绝服务(Distributed Denial of Service),是从 Dos(Denial of Service)的基础上发展而来的一种攻击方式,其运作原理是攻击方通过大量的数据包和目标服务器建立连接,占用目标服务器的宽带,导致目标服务器无法为正常的用户提供服务。若将受害系统比喻为餐饮店,将正常顾客进入店内点餐消费的行为理解为“系统的正常运行”,那么 DDoS 的工作原理就类似,命令不会消费的非正常顾客不断涌入餐饮店内,占用餐厅的空间资源,最终导致餐厅忙于处理非正常顾客的“刁难要求”,正常顾客既无法进入店内也无法消费,该餐厅实际上无法正常运转。具体案例参见北京市昌平区(县)人民法院(2021)京 0114 刑初 823 号刑事判决书等。

⑤ 如欧某某以免费观看 iCloud 黄色视频为诱饵,欺骗被害人登出手机 ID 后打开“查找我的 iPhone”功能,利用该功能锁定被害人手机,随后以解开手机为由向被害人索要 12282 元“开机费”。参见江苏省如东县人民法院(2020)苏 0623 刑初 311 号刑事判决书。

⑥ 江某某发现浙江某网络科技有限公司付款模块存在漏洞后在某商城平台下单。随后利用抓包软件抓取、修改报文数据修改该网络订单的支付数据,使得无需实际支付金额即可完成支付,某购商城平台收到修改后的订单数据后误认为该订单已经付款成功随即自动发货。参见浙江省杭州市余杭区(市)人民法院(2017)浙 0110 刑初 1308 号刑事判决书。

⑦ 王某某为逃避绵阳市安州区生态环境局的自动监测,私自篡改塔环境自动监测设备的取水管道和私接排水管道走向,同时将自动监测设备的采样水管插入装自来水的瓶中,干扰采样,致使自动上传至绵阳市安州区生态环境局的监测数据严重失真。参见四川省绵阳市安州区人民法院(2022)川 0724 刑初 12 号刑事判决书。

⑧ 长安某子站系国家环境保护部确定的空气质量监测站点。李某某、张某某多次进入站内,用棉纱堵塞采样器,干扰站内环境空气质量自动监测系统的数据采集功能,造成该站自动监测数据多次出现异常,多个时间段内监测数据严重失真,影响了国家环境空气质量自动监测系统正常运行。参见陕西省西安市中级人民法院(2016)陕 01 刑初 233 号刑事判决书。

果。这一观点背后隐含的逻辑是以评估结果的“正确性”判断系统运行的“正常性”。笔者认为,用自然语言意义上的“主观”目的判断代码逻辑意义上的“客观”运行状态并不合理,是实践对本罪的一种典型误读。判断系统运行结果的正确性存在客观与主观两套体系,以算式“2+3=5”为例,客观评价体系将系统视为处理数据的逻辑代码,认为系统的运行流程为“输入数据—处理数据—输出数据”,算式中“+”为系统的规则数据,决定系统的运算逻辑为加法;“2”“3”为输入数据,执行加法运算逻辑的具体规则。若行为人将规则数据改为“-”,则结果输出为“-1”;若行为人将输入数据改为“3”“3”,则输出结果为“6”,虽然最终输出的数值不同,但以上结果均是执行运算代码的应有之义,即“正确结果”。只有系统不依循相应运算逻辑运行或者外部条件使其无法依循运算逻辑进行时,才属于代码逻辑意义上的“结果失真”。主观评价体系则是在系统的输出结果上附着设立者的主观目的,是科技代码与自然语言的链接,如算式结果数值为“5”时代表空气质量为“优”,为“6”时代表空气质量为“良”。主观评价体系下评估系统本身是对现实的拟合,拟合程度的高低决定输出正确结果概率的高低,二者成正比关系。前述案例中的“失真结果”正是主观评价体系下对系统拟合程度的评判。但诚如前文分析,“错误结果”不仅与系统客观运行状态有关,还与程序技术是否高级、编程思想是否先进等其他因素相关,因此结果“正确与否”不是“系统是否正常运行”(法益侵害结果)的充分条件,其作为检测标准不具有形式逻辑的充分性。正是因为其将不具有法益侵害可能的行为纳入本罪规制才造成了实践中的“适用泛化”现象。

其次,本罪在行为定性评价上的扩张,即当一行为同时触犯本罪与他罪时,实务倾向只以本罪评价行为。在张某破坏计算机信息系统案①中,张某出于泄愤报复目的删除公司部分系统文件的行为一方面是对公司机器设备的毁坏,构成破坏生产经营罪;另一方面又造成了系统无法运行的结果,符合本罪的规定,一行为同时触犯两罪,理应被评价为想象竞合。但法院却仅评价本罪一罪,忽视了行为与他罪的竞合关系。忽视行为的他罪评价在破坏计算机信息系统行为的司法实务中较为普遍,背后可能的原因是本罪法定刑规定较重、罪量标准较低、跳过行为的评价阶段直接以本罪论处一般不存在裁判错误的问题。因此归根究底,本罪定性评价扩张的现象是罪量标准与法定刑严厉程度的不适配造成的。

最后,本罪在行为罪数评价上的扩张,数行为分别构成本罪与他罪且行为之间具有目的与手段的牵连关系时,一般仅以本罪评价。在廖某某破坏计算机信息系统案②中,行为人廖某某利用系统规则锁定手机致使系统无法使用的行为符合本罪规定,属于索财的“手段行为”;在前的欺骗行为与在后的敲诈勒索行为属于“目的行为”,目的行为与手段行为之间具有牵连关系,符合“处断的一罪”。合适的处理结论是,目的行为与手段行为分别构成两罪,但因存在牵连关系仅以重罪一罪论述。本案的裁判法院仅评价手段行为而忽视了目的行为,这是实务中“适用泛化”现象的另一缩影。这一现象背后的原因同样是本罪的法定刑与罪量要求难以适配,即使跳过牵连评价过程也不存在最终裁判结果的差异,因此实务部门往往出于认定的便利或定案的惰性直接以本罪评价。《刑法》286条3款均规定只有行为符合“后果严重”规定才可构成本罪,“后果特别严重”可以成立加重犯,一般认为“后果严重”“后果特别严重”为罪量要素。《最高人民法院、最高人民检察院关于办理危害计算机信息系统安全刑事案件应用法律若干问题的解释》(以下简称《计算机解释》)第4条、第6条以列举方式规定了本罪罪量标准的具体内容,有学者认为该规定确定的入罪标准过低。[3]一个明显的例证是《计算机解释》第

① 张某原系被害单位员工,因对解除劳动合同一事心怀不满,在某地通过软件登录云服务器,使用管理员身份进入公司自有服务器与租赁服务器并删除部分系统文件,导致公司官网等系统自2017年7月5日16时许开始不能访问,至2017年7月10日上午11时许才恢复正常运行。经核算,截至2017年7月4日之前,公司系统有超过16212名以上的用户。参见北京市海淀区人民法院(2019)京0108刑初1364号刑事判决书。

② 2018年12月至2019年1月间,廖某某伙同他人共同在“王者荣耀”游戏中谎称帮其升级游戏人物可以免费赠送游戏皮肤,诱骗被害人等使用其提供的ID及密码登录苹果手机。廖某某再利用苹果手机相关功能远程锁定被害人的苹果手机,后再通过网络聊天软件与被害人联系,以解锁为条件索要财物。行为人共计作案10起,索得财物合计人民币1400余元。参见江苏省苏州市相城区人民法院(2020)苏0507刑初50号刑事判决书。

4 条第 1 款规定，违法所得 2.5 万元以上就符合“后果特别严重”的要求，同样作为破坏型犯罪的故意毁坏财物罪却要求 5 万元才符合“数额巨大”。二者相比，破坏计算机信息系统罪的罪量显然畸轻。除此之外，《计算机解释》还规定破坏 10 台计算机信息系统即可成立犯罪，这一规定也显然不适应当下“端网泛化”的情态，存在罪量标准要求过低的嫌疑。

简言之，实践中存在的“适用泛化”问题是本罪行为之“质”未被明确且修饰“质”的罪量标准过于宽泛造成的。换言之，本罪的罪量标准亟待进一步明确。为解决本罪适用泛化问题，落实罪刑法定原则，需要在教义学层面对其进行更深入、系统、全面的剖解与重塑。

二、破坏计算机信息系统罪罪量要素的体系定位

根据我国刑法的规定，在具备类型化行为与危害结果本身的不法之外，成立犯罪还需达到危害程度（“量”）的要求，形成了独有的“定性+定量”刑事立法模式。本罪立法中的“后果严重”“后果特别严重”就是以明文形式存在的“量”的要素，类型行为只有满足“后果严重”指涉的不法含量才可能成立本罪。罪量要素的体系定位一直为学界所争议，不同的体系定位必然带来界定罪量内容的不同标准，但“倘若人们不正确地构建或者安排了刑法体系的要素，那么，就有可能导致有缺陷的结果”[4]。由此，需要首先在教义学层面展开对罪量要素体系定位的考察。

（一）“类构成要件复合体”：本罪罪量要素的实然定位

《计算机解释》第 4 条规定了本罪第 1 款、第 2 款罪量要素的具体内容，主要涉及以下几个方面：行为对象（系统）的重要程度、行为对象的数量、违法所得或经济损失数额、危害结果累计时长、社会影响。其中行为对象的规定是对行为不法程度的修饰，而“经济损失数额”“危害结果累计时长”则是对结果不法程度的修饰，根据学者观点，二者皆处于构成要件的不法量域内。[5]而“违法所得”因与法益侵害不存在关联被评价为不法中立的“真正的客观处罚条件”；[6]“社会影响”“生产、生活影响”是行为造成的二次加重结果，其在一定程度上征表着法益侵害的严重程度，因而不属于“真正的客观处罚条件”，但该结果与破坏行为之间又不必然存在刑法上的因果关系，学者将其中由行为偶然、异常造成的部分称为“不真正的客观处罚条件”[7]、“客观的超过要素”[8]或“内在的客观处罚条件”[9]。

笔者认为，实然状态下本罪的罪量要素更接近王莹教授提出的“类构成要件复合体”，[10]既存在构成要件量域内的标准，又有超出构成要件之外的真正与不真正的客观处罚条件。① 虽然司法解释是对实务的指导，但并不意味着学者需要在刑法教义学上为这一现实寻觅合理依据，相反，坚守本心，对僭越立法的司法解释保持批判立场才是刑法教义学的存在之本。诚然，“违法所得”标准或许存在诉讼证明便利等好处，但教义学也不能仅仅为刑事诉讼效率考虑而忽视其实体法上对法益侵害原则的背反。在统一界定“后果严重”的范围以实现司法统一适用、解决本罪适用泛化问题的立场上，笔者认为本罪罪量要素的体系定位为“典型的构成要件要素”，其外延应仅限构成要件的基本不法量域，“真正的客观处罚条件”“客观的超过要素”不被涵括在内。

（二）“典型的构成要件要素”：本罪罪量要素的应然选择

构成要件要素内部存在“典型的构成要件要素”与“非典型的构成要件要素”两种类型，后者又被称作“客观的超过要素”“不真正的客观处罚条件”等。“客观的超过要素”系张明楷教授为明晰丢失枪支不报罪等犯罪的主观罪过形式而创设性地提出的概念，指涉刑法规定中属于构成要件要素但无需行为人有所认识的内容。[11]但当客观的超过要素内容与行为的不法程度存在关联时，张明楷教授认为行为人应至少具有预见可能

① 王强教授在犯罪成立说的立场下谈论客观处罚条件，认为真正的客观处罚条件是“立于违法与责任之外的，决定犯罪成立的真正的客观处罚条件”，如作为犯罪报酬的违法所得数额；而不真正的客观处罚条件则属于非典型的构成要件要素，在犯罪论体系中处于“该当性”范畴，如“致使（当事人或近亲属）自杀、自残”等情节要素。王莹教授则认为“被害人自杀、自伤”后果与行为人的行为不具有刑法上的因果关系，因此属于“溢出构成要件”的客观处罚条件。虽然二者在客观处罚条件的内容与体系定位上存在差异，但均认同客观处罚条件实际上具有独立影响犯罪成立的地位。下文中所用“客观处罚条件”一词是在王莹教授确定的独立影响犯罪成立地位的意义上使用的，其地位等同王强教授认为的“真正的客观处罚条件”。

性。[12]本文认为,本罪“后果严重”不是“客观的超过要素”,主要存在两点理由:一方面,“客观的超过要素”说本身与责任原则龃龉,其理论内容本身尚存疑。作为与不法内涵关联的要件,为何“客观的超过要素”能够超然故意的认识内容之外?同时,客观的超过要素与典型的客观构成要件要素间主观认识的差别也缺少合理论据。① 另一方面,《刑法》第286条规定本罪的后果要件是“计算机信息系统无法正常运行”“影响计算机信息系统正常运行”等妨碍系统运行的情状,“后果严重”作为紧随危害后果的修饰定语,修饰作用决定了其应仅为填充后果严重程度的具体细则。作为纵向依附这一危害之“质”的程度标准,其内容上应与行为保持刑法上的因果关系,即归因于第三人行为的结果要素无法被涵括在内,这是形式逻辑的自然推演结论。此外,在修饰“此质”的“量”下附着“他质”内容也易造成此罪与彼罪的混淆。

因此,本文认为,“后果严重”是典型的构成要件要素,主要理由是将“后果严重”认定为典型的构成要件要素有助于缓解实践中的“适用泛化”现象。如前文所述,罪量标准过低是导致本罪“适用泛化”的重要原因。将“后果严重”认定为典型的构成要件要素,排除其间属于真正的客观处罚条件、客观的超过要素的能指,实现本罪罪量要素所指内容的限缩;本罪为故意犯罪,行为人的主观认知范围当然及于作为客观构成要件要素的严重后果,如此便可提高本罪实务适用的证明难度,达到缩减适用的目的。

根据构成要件理论,故意认识的范围涵盖本罪的客观构成要件,“后果严重”所指涉的事实当然成为本罪故意认识的内容。但这一事实的规范评价是否要求行为人有所认识及需要认识到何种程度,学界存在不同观点。② 本文认为“后果”为事实性要素,“严重”则为规范性评价,“严重”作为对“后果”的修饰,本身包含刑事立法中的价值倾向,绝非单纯的事实描述。确认“后果”指涉事实的过程属于事实判断,但“后果是否严重”则是涉及价值判断始能加以确认的情形。据此,应当认为“后果严重”属于规范性的构成要件要素,[13]行为人在认识作为基础事实之“后果”后也需要对规范评价有所认识,但无需明晰其法律概念或含义,只需认识到行为的规范评价达至社会一般人认为的严重即可。[14]

“规范的构成要件要素说”对行为人的主观认识提出了两点要求:第一,认识事实,即“后果”;第二,认识基础事实的规范评价,即“后果”应达至社会一般人评价的严重程度。只有满足二者才成立故意犯罪,缺少二者其一即阻却犯罪故意成立。在宁某某、代某某破坏计算机信息系统案③中,行为人对破坏计算机信息系统数量的认知限于犯罪行为的直接对象,即41台“客户端”,对借由“外挂软件”成功上网的4436台“用户端”数量不存在基础事实的认知,属于事实认识错误,应当阻却加重犯故意的成立,行为仅符合本罪基本犯的规定。

综上所述,本罪罪量要素属于典型的构成要件要素。据此我们可以得到主观与客观的两条教义学限制:客观上,“后果严重”内容横向征表行为侵害法益的严重程度,纵向紧附于与行为存在刑法上因果关系的危害结果;主观上,行为人需认识到“结果”依托的基础事实与评价结果的价值结论,但对后者的认识只需要达至社会一般人认为的严重程度即可。

三、破坏计算机信息系统罪的法益厘清

罪量要素是行为法益侵害程度的征表,限缩本

① 故意犯罪要求行为人明确认识客观的构成要件要素,张明楷教授认为针对“客观的超过要素”行为人只需“具有预见可能性”即可,二者差别的合理性存疑。

② 主要存在两种观点,即“事实的构成要件要素说”“规范的构成要件要素说”。前者认为认定相关的故意要求行为人对“情节”与“严重”均有所认识,对“情节严重”的认识错误属于事实认识错误,影响故意的认定。参见余双彪.论犯罪构成要件要素的“情节严重”[J].中国刑事法杂志,2013(8):33-34。后者则采取“外行人的平行评价公式”,要求行为人站在外行人的领域或立场,认识到构成要件要素的基础事实及其社会意义即可。参见张明楷.犯罪构成体系与构成要件要素[M].北京:北京大学出版社,2010.239。

③ 宁某某以人民币1000元的价格从他人处购买“电脑医生”外挂软件,该软件可通过破坏公安部核发许可的“iKeeper网络安全管理系统”,规避我国关于网吧实名制上网的强制性规定。2012年10月,宁某某在代某某的帮助下获得该软件的永久使用权。此后,二人分别以500元至1300元不等的价格通过互联网销售该软件。截至案发,二人分别向41家网吧销售该软件,涉案电脑4436台。一审法院认为行为人破坏41台计算机信息系统的实名上网监管功能,两行为人成立286条第1款基本犯罪;抗诉机关则认为该案涉及的4436台计算机系统的实名制上网监管程序均遭到破坏,行为人行为属于加重犯,一审判决的宣告刑畸轻。参见宁夏回族自治区银川市中级人民法院(2015)银刑终字第182号刑事判决书。

罪罪量要素的具体内容需要首先明确本罪的法益内涵。关于本罪法益的具体内涵,学界存在“国家对计算机信息系统的管理秩序”(下简称“管理秩序说”)“系统的正常运行与数据的完整性说”(下简称“双法益说”)“系统的完整性与可用性说”“计算机信息系统的正常运行说”(下简称“正常运行说”)等观点,笔者赞同“正常运行说”。

(一)“正常运行说”之提倡

首先,本罪的法益不适用“管理秩序说”。学界有观点认为本罪的保护法益是国家对计算机信息系统的管理秩序。[15]该观点也得到了部分实务判例的支持。① 管理秩序说认为个罪法益理应被涵括于类罪之内,“章—节—条”的表现形式并不仅限于简单的外观,而实质征表三者法益内涵存在包容关系,是体系解释的应然结论。这种观点虽具有一定合理性,但却忽视了教义学理论对立法规定的检视机能,即越过了管理秩序能否成为适格法益的检验步骤。

本文认为,国家对计算机信息系统的管理秩序无法成为本罪法益,主要有以下几点理由:第一,管理秩序不是适格法益。根据日本学者伊东研祐提出的共识性的法益概念,“法益是指所在国家的宪法构成(应该)的社会内,作为该社会构成成员共同生活的存立必不可少的条件,而且是由纯粹规范所保护(应该)的因果性变更可能的对象。”[16]这里至少提出了“某种利益”合理上升为“适格法益”的两点要求:人们共同生活存立必不可少的要件;因果性变更可能的对象。前者要求这种利益必须是规范之前就已存在的、真实的生活利益,而非被规范保护之后的表象产物,且属于促进人格发展的条件;后者要求这种利益客观上有可能受到损害或威胁。“管理秩序”包括两个方面内容,即客观上不被侵害的状态与主观上相信不被侵害的信赖,前者是规范效力的体现,后者则是民众对规范效力的信赖,二者均是法益被保护后呈现的表象结果,并非先于规范的实存,无法与既存规范分离。除此之外,法益保护结果更多惠及以国家为代表的机关或组织等集体,与个人关联较弱,因此管理秩序也难被称为“促进个人社会发展的条件”。综上所述,计算机信息系统的管理秩序能否成为适格法益尚且存疑。但即使忽略前述检验结论,管理秩序说还存在一个不可忽视的缺点,即因语义模糊导致的无法发挥解释构成要件机能,易引发滥用司法自由裁量权的问题。[17]这意味着其无力解决实践中的“适用泛化”问题,与本文的应然目标相悖。换言之,即使可能成为法益,管理秩序说也并非适合本罪当下实务语境的法益。第二,管理秩序说无法在规范文本中找到存在依据。法条文本的文义形式蕴含着立法最初的规范保护目的。[18]从罪状描述来看,规范主要着眼系统本身的性质,保护系统技术运行的实现。第 1 款与第 3 款规定的“无法正常运行”也是围绕系统本身,而非主体对设备的控制关系。若将保护视野扩大至“主体—设备”关系将产生此罪与彼罪,尤其是本罪与控制计算机信息系统罪的混淆,造成本罪适用的进一步泛化。此外,学界似乎存在体系定位决定个罪法益的看法。笔者认为,章节体系确定罪名法益的作用应该是指导性的,但并非绝对、唯一的,且个罪法益也绝不应当照搬章节类罪法益,而应立足现状从规范表述生发,以实践所需为锚点确定。即使为平衡体系,法益也只需与“社会秩序”存在一定程度的勾连即可。

其次,认为本罪第 2 款为数据安全法益的“双法益说”也不具有合理性。[19]第一,双法益说将本罪前两款规范保护目的割裂开来,与规范目的的体系统合功能相悖。双法益说认为本罪第 1 款保护“系统的正常运行”,第 2 款保护“数据的可用性与秘密性”。前者聚焦具体设备,属于“系统视角”;后者则聚焦数据要素,是区别于前者的“数据视角”。囿于科技的发展,立法者制定本罪所依托的模型仍然是“设备—系统—数据”的计算机最简模型,[20]最简模型下的数据被存储在计算机中,三者含义可以等同。但在“云存储”“云计算”等云端、雾端技术发展的当下,系统(计算能力)与数据都逐渐脱离物理设备成为独立的维度,三者含义无法等同。因此,对系统的保护应区别于另外两者,即数据安全与系统安全应分属不同的保护领域,不可混淆在同一罪名内。目前学界大多认为《刑法》第 285 条非法获取计算机信息系统数据罪及其他非法获取信息或者机密类的

① 如福州市中级人民法院在“陈某破坏计算机信息系统案”二审判决书中明确,“本案以计算机信息系统数据为犯罪对象,侵犯的客体主要是计算机信息系统管理秩序”。参见福建省福州市中级人民法(2016)闽 01 刑终 643 号刑事判决书。

犯罪可能属于保护数据内容的犯罪。“数据—系统”的双层次保护模式体现了数据作为“内容—载体”的一体两面。前者将数据视为“权利束”,关注数据内容的现实性,以其表征内容甄别行为性质[21];后者则将数据视为“计算资源”,关注数据运算的虚拟性,行为破坏系统运行安全成为应罚本质[22]。二者拥有不同的侧重点及保护目的,分属不同保护层次。[23]将二者混同会不当减缩系统安全的保护范围,同时产生“数据—系统”双层次保护体系罪名适用域围的不当交叉,导致刑事法规无法发挥裁判机能。第二,即使忽略体系美感的要求,“数据的完整性与可用性”还会因外延过大导致实践适用的进一步泛化。数据在技术上仅表现为 01 进制字符,而任何电脑操作都可被认为是对 01 字符的“删除、修改、增加”,那么任何单一的无权或越权电脑操作行为均已符合本罪“质”的可罚性,即使行为人删除文档单个字符的行为也不例外。这无疑大大增加了本罪适用的可能,与限制本罪适用的原初目标背道而驰。与第 1 款与第 3 款相比,本罪第 2 款并没有明确规定“造成计算机信息系统无法正常运行”。双法益的支持论者认为这一差异不是立法者的疏漏,而是其有意为之,旨在表明本罪第 2 款保护的利益区别于前后两款,是立法者对双法益说持支持态度的有力证据。[24]本文认为这一“证据”仅为教义学层面的解读,含有学者的主观揣测,难言“有力”,此外其忽略了数据法益背后刑事可罚范围过大的隐患,也背离了法益论自由主义机能的初衷。[25]

再次,“系统的完整性与可用性说”也无法成为本罪法益。依据论者描述,系统的完整性为“不因人为的因素而改变网络信息原有的内容、形式和流向”[26],保护范围包括数据与应用系统。具言之,系统完整性包括数据的完整性与应用系统的完整性,破坏二者其一即认为系统完整性造成了破坏。这种含义下的“系统的完整性”等同于“数据的完整性”,其同样存在犯罪圈过大的问题。此外,破坏数据与破坏数据有机组合体(应用程序)明显存在违法程度的区别,理论上应当设置不同的法定刑,但实际立法却相反,支持者也未对这一明显矛盾作出解释。同时,系统的可用性为“按照授权实体的要求可被访问和可被使用的性质”[27],即包括可被访问与可被使用两部分。笔者认为,“可被访问与可被使用”这一状态的实现需要系统本身处于可以被访问的状态及相关权利人拥有访问权限两个条件,前者符合本罪规范保护目的,后者则关涉其他利益主体对设备的控制权限,因而落入非法控制计算机信息系统罪的保护范围。此外,论者仿照“数据的完整性与可用性”的含义确定“系统的完整性与可用性”,仅将主语作简单替换。“数据安全”视角下的数据是虚拟层面的最小元素,类似生物学的“细胞”,而“系统安全”视角更侧重系统的运行,类似于“组织”。二者本身存在视野的差异,强行嫁接在一起忽视了二者量级的不相容,反而造成犯罪圈的进一步扩张。

最后,本罪法益应采用“正常运行说”。一方面,其为立法者明确表示。《〈中华人民共和国刑法〉条文说明、立法理由及相关规定》将本罪的立法理由表述为“保障计算机信息系统安全和功能的正常发挥,维护计算机信息系统安全运行,违反国家规定,破坏计算机信息系统功能,后果严重的行为,有必要予以刑事制裁……”[28]可见,“正常运行说”符合立法者最初的设立目的。另一方面,将法益限定为“系统正常运行”是对系统安全的保护,能够与数据维度下的数据安全区分开来,实现“数据—系统”的双层次规制模式。

有学者提出将第 2 款法益认定为“系统的正常运行”会造成“第一款规定完全包含了第二款规定”[29],违反了刑事立法的无赘言原则。本文认为上述问题完全可以通过区分数据类型解决,且为立法区隔直接破坏行为与间接破坏行为的表现。将计算机信息系统理解为依循代码逻辑处理数据的有机体,这一有机体内存在两种数据类型:一为“规则数据”,即设定系统如何处理、存储、传输数据的代码,而依照这一“游戏规则”运行的要素则被称之为“内容数据”。增加、删除或修改规则数据当然存在极大概率造成系统无法正常运行,因此作为典型的行为样态被固定在本罪第 1 款中;但操作内容数据同样可以达到系统无法正常运行的结果,例如 DDoS 行为通过占用系统有限资源,导致系统一直忙于处理干扰因素而无法处理正常请求,造成系统网速下降、网页崩溃,无法正常运行。以规则数据为对象的删除、修改或增加是针对系统的直接破坏,而通过删除、修改或增加内容数据造成系统无法正常运行则是利用系统规则的“作弊”行为,属于间接破坏。虽然最终

都造成了系统无法运行的外观，但二者破坏方式存在显著差别，由不同款项分别规制。具言之，确定“删除、修改、增加数据，造成系统无法正常运行”行为的适用时，若行为对象为“规则数据”则适用第 1 款，若行为对象为“内容数据”则适用第 2 款。第 2 款当然无法被包括在第 1 款中，两款之间的包含问题也不复存在。

（二）“正常运行说”之具体内涵

确定法益后，还需进一步厘清其含义。笔者以“用户重要的计算机数据和资料遭到不可恢复的严重破坏”[30]标准与最高人民法院第 104 号指导案例确立的“结果是真与否”标准为坐标轴的两端，通过逐一分析坐落其中的其他情景，在行为类型中寻找本罪结果的大致坐标，确定危害结果的不法区间。

第 104 号指导案例以棉纱堵住漏网的外部干扰行为导致结果失真为由，认定空气监测系统没有正常运行，进而判定行为人构成破坏计算机信息系统罪。但所谓的“外部干扰”是对设备外部物理环境的扰乱或更改，并不以虚拟层面的数据为对象，也并未出现系统崩溃、网速下降等系统无法运行等结果表征，因此笔者认为其并未造成系统无法正常运行。相反，“失真的结果”恰恰是系统正常地依循规则逻辑运行的体现，换言之，即使结果失真亦无法代表系统运行安全受损，因此这种标准下的结果具有较低的不法含量。与此相反，有些学者认为本罪结果必须为“不可恢复的严重破坏”，这又走向了过高要求危害结果不法含量的另一误区。

笔者认为不能极端理解“无法正常运行”，其在现实中的合理指涉应处于上述两端中间地带的某处，这一地带上恰巧分布着实践中颇具争议的 4 类行为（图 1 中间 4 类行为，从左至右不法程度依次递增）。本文通过对比类型结果与规范语词，在“目光不断流转于规范与事实”中逐渐接近规范语词含义的中心地带，以确定本罪结果的大致样态，进而明晰本罪危害结果“质”的不法区间。

4 类行为分别是：第一，“单纯地”删除、修改、增加数据的行为，实务中常表现为删除、修改或增加学校教学科研系统中的师生信息、警务系统中的违章记录、电商平台的评价记录等；第二，删除、修改或增加“指令”等内容数据但未对系统运行效率产生影响，实务中常见行为样态是 Fiddler 抓包；第三，删除、修改或增加内容数据且影响系统运行效率的行为，常见案例为 DDoS 行为；第四，删除、修改或增加内容数据，利用系统规则致使系统锁定、无法使用的行为，常见为欺骗被害人登出苹果 ID 账号后利用“查找功能”锁定苹果手机，向受害人索取“解锁费”获利的情形。第一种行为与第二种行为是广义的非法控制计算机信息系统的行为，①并未影响系统的正常运行；第三种行为对系统的运行效率产生了影响；第四种行为则造成了系统锁定、无法运行的后果。

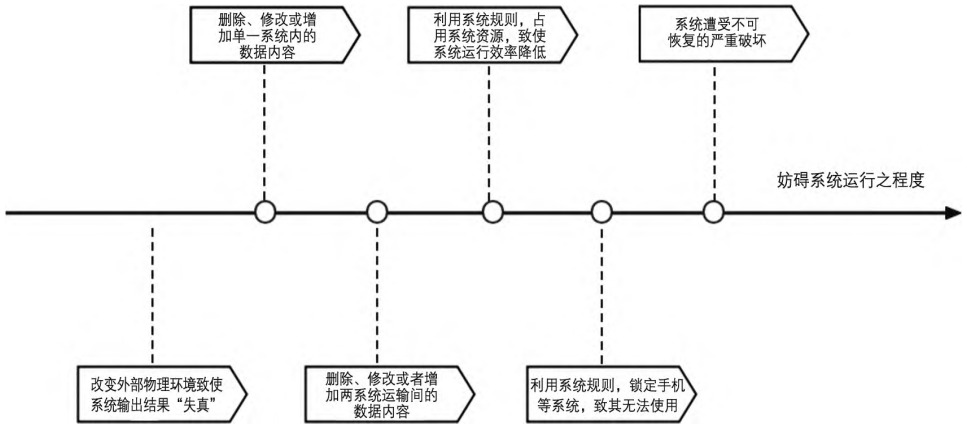

图 1　妨碍系统运行程度指示图

① 最高人民法院大法官胡云腾，学者皮勇等人均认为“非法控制”存在广义与狭义之分。广义上，未经授权或者超越权限的系统操作行为均属于“非法控制”，而狭义的“非法控制”则强调完全排除相关权利人对系统的占有，是一种针对系统的破坏行为。参见胡云腾. 网络犯罪刑事诉讼程序意见暨相关司法解释理解与适用[M]. 北京：民法院出版社，2014. 109. 94-95；皮勇. 我国网络犯罪刑法立法研究——兼论我国刑法修正案（七）中的网络犯罪立法[J]. 河北法学，2009（6）：53。此处采取的是广义上“非法控制”含义，只要求相应的越权操作行为，不要求完全排除权利人的占有。

下面通过具体案例分别对上述4类行为予以阐释。在郑某某破坏计算机信息系统案①中,郑某某系在单一系统终端内修改内容数据;在李某某破坏计算机信息系统案②中,李某某是在数据往返两终端的运输过程中修改数据内容。二者行为的发生场域不同,但均未对系统运行状态产生妨碍。前者而言,系统依照规则完整展现违规录入的住址信息,数据信息的完满展示正是系统依照规则正常运行之结果;后者而言,系统的输出结果依照输入数据的变化而变化,但产出结果的运算逻辑仍然相同,且系统本身的运行速度与程序运行的外在环境亦未受妨碍。系统在接受"充值0.01元"的指令后依照规则输出"XX用户到账金额为0.01元"的结果指令,数据更改没有妨碍造成系统运行之可能,行为时系统处于正常的运行状态中。综上,不能认为单纯修改或更换数据但未影响系统正常运行之可能的行为符合本罪危害结果之规定。

在万某某破坏计算机信息系统案③中,DDoS攻击行为通过向目标系统不断发送请求,占用系统合理资源。这一过程减缓系统的运行效率,是对系统正常运行的妨碍。与前述两案例相同,系统正是因为遵循规则数据确定的处理原则才导致其不断回应"错误请求",最终造成资源耗尽的后果,虽然规则数据同样未受影响,但系统运行状态却受到了妨碍,具体表现是出现了"系统没有流量"等外显后果。虽然其未删除、修改或者增加系统的规则数据,但仍对系统运行状态有所影响,属于间接破坏系统运行安全的行为。

而在陈某某破坏计算机信息系统案④中,陈某某系利用系统规则破坏系统运行。有学者认为利用系统规则的行为不属于"破坏",因为系统本身完好无损。[31] 笔者认为,破坏计算机信息系统罪3款规定暗含了系统正常运行的3个条件:系统运行规则本身完整、圆满,未受更改或者破坏;系统处于"正确"的运行方向,运行效率无虞;系统所处平台拥有良好的运行环境,免受病毒等破坏程序干扰。支持论者认为系统规则完好无损即代表系统处于良好运行状态的观点只注意到了维持运转所需的一个面向,忽视了其余二者。况且,从"系统无法运行"的形式解释出发,"手机无法开机"当然涵括在"系统无法运行"的外延内,甚至是词语含义的典型表现。否认这一表现反而会损害国民稳定的法感情,违背罪刑法定原则,带来罪责刑不相适应等问题。

综上所述,处于两端光标中间地带的"系统无法正常运行"外在结果至少应表现为系统运行状态的某种可视妨碍;内在行为可以是删改增规则数据,也可以是影响系统的运行方向或系统所处的运行环境,同时妨碍结果需可归因于虚拟层面的行为。只有满足外在结果、内在行为与因果关系三个条件,才可认为案例中的结果要素确实属于法条规定的"系统无法正常运行"。

四、破坏计算机信息系统罪罪量标准的展开

确定本罪危害结果后,我们即可得到"量"所依附的"质"。《计算机解释》针对实践中出现较多的第1款、第2款行为,主要从以下几个方面规定了本罪的罪量标准:行为对象(系统)的重要程度、行为对象的数量、违法所得或经济损失数额、危害结果累计时长与社会影响等。本文认为,"违法所得"标准属于客观处罚条件,与违法本质无涉,应当予以排除;"社会影响"标准外延较广,

① 因在温州购买车牌需要在计算机系统内查询相关住址信息,潘某某要求原担任街道全科网格员的郑某某将其提供的身份信息违规录入浙江省流动人口管理系统,以实现请托人办理车牌的目的,郑某某照做,事后两人通过收受请托人好处费获利。参见浙江省乐清市人民法院(2020)浙0382刑初540号刑事判决书。

② 李某某发现河南某商业股份有限公司APP在线充值平台存在漏洞,遂在该平台注册用户进行充值测试。利用"Fiddler"软件拦截在线充值平台发送的数据包,将支付金额指令内容(数据)由"1000元"修改为"0.01元",最终其只支付0.01元,但APP实际到账"1000元"。此后,李某某重复上述步骤在APP内进行多次充值,共计操作108次,支付1.08元,实际充值账户金额为108000元。参见河南省郑州市高新技术产业开发区人民法院(2020)豫0191刑初1243号刑事判决书。

③ 南通X网络科技有限公司(以下简称"X公司")系家纺销售电子商务类民营企业。X公司法定代表人万某某因怀疑竞争对手J公司攻击了自己公司的网站,与技术总监杨某某等人商议后决定雇佣黑客攻击J公司网站(该网站为1万以上用户提供服务)。万某某雇佣刘某攻击J公司网站,刘某雇佣朱某等人共同对J公司网站进行DDoS攻击,导致网站租用的服务器被封堵,J公司网站于当日17时15分至18时30分没有流量、不能正常运行。最高人民检察院.检察机关依法惩治破坏市场竞争秩序犯罪典型案例[EB/OL].https://www.spp.gov.cn/spp/xwfbh/wsfbt/202208/t20220804_569841.shtml#2.

④ 陈某某于2019年5月至7月间多次通过QQ群发布虚假招嫖信息的手段结识被害人,以提供"小妹照片"为幌子,诱骗被害人登陆特定苹果ID。待被害人登录后利用苹果系统自带的"查找手机"规则锁死苹果手机,再以解锁手机、收取服务费等各种理由迫使多名被害人转账、扫码支付等交付人民币5600余元以上。参见江苏省常熟市人民法院(2020)苏0581刑初203号刑事判决书。

应当通过剔除其中的“客观超过要素”限定其内容;“直接经济损失”标准与行为危害程度存在关联,但需严格解释;“时长”标准具有一定合理性,在适当语境下可以扩张适用。

(一)排除“违法所得”标准

除却本身与不法无涉,不属于“典型的构成要件要素”外,“违法所得”标准本身还具有较大的偶然性与变动性。在最高人民法院指导案例 103 号徐某破坏计算机信息系统案中①,徐某前后分别实施两次行为:第一次行为破坏 4 台计算机信息系统,收受违法所得 3 万元;第二次破坏 1 台计算机信息系统,违法所得 1.5 万元。依照“台数”标准,行为人前后行为尚未成立犯罪,但若依照“违法所得”标准,行为人却成立本罪的加重犯。上述结论矛盾的原因是,“违法所得”是取决于交易主体、交易场域、甚至双方社会关系的主观标准,具有较大的偶然性与不确定性。以与不法无关的“违法所得金额”决定犯罪成立,就会出现行为拥有完全相同的罪质,仅因交易的偶然不同就出现大相径庭的结论,是不被现代刑法理论接受的。因此,“违法所得”标准应被排除在罪量内容之外。

(二)具化“社会影响”标准

《计算机解释》第 4 条第 2 款第 3 项规定,“破坏国家机关或者金融、电信、交通、教育、医疗、能源等领域提供公共服务的计算机信息系统的功能、数据或者应用程序,致使生产、生活受到严重影响或者造成恶劣社会影响的”属于“后果特别严重”,构成本罪的加重犯,笔者称其为“社会影响”标准。第 3 项采用“行为对象+行为结果”的规定方式,行为对象是关乎民生的公共计算机信息系统,是行为不法含量的直接表征;“严重的社会影响”也与不法存在一定程度的关联,是行为的二次结果、危害结果的次生危害,间接征表“质”的不法程度。“严重的社会影响”与行为之间并非刑法上的因果关系,可能存在第三人行为的阻断。笔者认为,应当具化“社会影响”内涵,将其限定在与行为具有刑法因果关系的外延内。同时,行为以“二次结果”作为罪量要素,本应是限制加重犯成立的表现,但“社会影响”“严重”“恶劣”等词语却因不明的语义、模糊的标准使得罪量要素事实上成为降低入罪门槛的助推,反而增加了本罪适用的可能。为正本清源,发挥其应有的限制功能,应当紧紧围绕词语的核心语义,通过指导案例明确本标准在实务中的具体类型,在本罪间的横向类比与他罪的纵向对比中不断提炼、校准本标准的模型特点,并推广适用。首先,应明确“二次结果”的体系定位,只有“无法正常运行”的结果出现后才可进入是否符合“二次结果”的判断;其次,应抛却司法中“案件知名度”等依靠法感情判断的标准,为“生产、生活影响”“社会影响”注入更多客观可触的内涵。

(三)严格解释“经济损失”标准

司法解释规定造成经济损失 1 万元以上的应当认定为后果严重,同时规定经济损失是指“危害计算机信息系统犯罪行为给用户直接造成的经济损失,以及用户为恢复数据、功能而支出的必要费用”。这一定义包含了两部分的内容,二者应并行适用。此处争议较多的是应如何认定“直接经济损失”。如在罗某某破坏计算机信息系统案②中,行为人向俱乐部有限公司赔付的 3 万元系行为造成的直接后果,可以认定为直接损失。较有争议的是 B 提出的总价 30 万元的赔偿与 C

① 钟某某发现其购得的泵车即将被中联重科锁机后,安排徐某 1 帮忙打听解锁人。徐某 1 遂联系龚某某告知钟某某泵车需解锁一事。龚某某表示同意后,即通过电话联系徐某 2 给泵车解锁,当日及次日,龚某某还带着徐某 2 为其管理的其妹夫黄某以分期付款方式购得的牌号分别为三台泵车进行永久解锁,事后龚某某向被告人徐某 2 支付解锁费用共计人民币 30000 元。张某某因拖欠货款,泵车被公司锁定无法正常作业,张某某遂通过电话联系徐某 2 为其泵车解锁。被告人徐某 2 采用上述同样的方式为张某某名下泵车解锁。事后,张某某向被告人徐强支付解锁费用 1.5 万元。经鉴定,泵车 GPS 终端被拆除及控制程序被修改后,中联重科物联网 GPS 信息服务系统无法对泵车进行实时监控和远程锁车。参见最高人民法院指导案例 103 号:徐某破坏计算机信息系统案[湖南省长沙市中级人民法院(2016)湘 01 刑终 58 号刑事判决书]。

② 罗某某在宣某公司负责平台数据编写和维护工作。因对离职待遇不满,为报复公司,罗某某编写脚本,利用其在公司工作时得到的公司账号密码,将公司存放于阿里云服务器的后台数据进行删除,共删除图片 1300 张(约 4.7G 被清空),造成合作方深圳市某游艇俱乐部有限公司的选手图片无法显示,无法进行有效点击。案发后,宣某公司向深圳市某游艇俱乐部有限公司(下简称俱乐部有限公司)赔付经济损失人民币 3 万元,罗某某家属代为向宣美公司赔偿人民币 3 万元,并取得谅解。其余使用同一投票系统的两家合作方(下简称 B)提出,若宣某公司无法及时修补系统,找回丢失图片信息,恢复系统正常运行,则要求宣某公司分别赔偿 15 万元。另一合作公司(下简称 C)向宣某公司要求的损失金额为 13 万余元,但其随后又表示,因宣美公司积极补救损失具体赔偿另行协商。同时依据被害单位法定代表人周某的陈述,被害单位在恢复、收集被删除的图片上并未支出必要费用。参见广东省深圳市福田区人民法院(2020)粤 0304 刑初 664 号刑事判决书。

在先提出的13万损失是否属于直接的经济损失?本文认为B提出的赔偿尚处于未确定的法律状态中,若条件未成就,宣某公司无需支付该款项。将尚处于未然状态的赔偿认定为“直接经济损失”显然不符合法理。即使后续宣某公司不积极采取措施恢复数据最终导致其向该两家合作方赔偿,此损失也不能完全归因于罗某的行为。C本身没有确定具体的赔偿数额,将处于变动状态的金额认定为直接损失有违“直接经济损失”背后的已然逻辑。因此本案中的直接损失仅限已经赔付的3万元。

《刑法》并未直接规定“直接经济损失”的具体内涵,立法缺位时应依法理补齐相关内容,以为实践适用指明方向。笔者认为实务确定“直接经济损失”时应大致遵循以下思路:首先考虑及时恢复系统运行而支出的必要费用,因为破坏后首先应考虑恢复。此处需格外注意费用范围以“必要”为限,为恢复花费的额外费用不在此列。其次,系统被彻底毁损无法恢复时应将重新制作的替代性费用理解为“直接损失”。“替身”需以“原本”为对照,若行为人趁机将系统迭代升级,则“直接损失”数额应将“原本”与“替身”之间的差价剔除。最后,若穷尽合理合法手段后仍无法恢复或重新制作,被害人确已无法履行合同时,以合同赔偿的金额为标准,且金额范围应以实然的直接损失为限,不包括可得利益等损失。

(四)适度扩张适用“时长”标准

《计算机解释》第4条第1款第4项前段规定“造成为一百台以上计算机信息系统提供域名解析、身份认证、计费等基础服务的”属于本罪规定的“后果严重”,同时第1项中规定“造成十台以上计算机信息系统的主要软件或者硬件不能正常运行的”也符合本罪“后果严重”的规定(见下表)。

表1 行为的不法程度对比表

	涉系统数量的最小值(台)	系统功能重要程度
第1项	10	基础服务
第4项	100	主要功能

由于“域名解析、身份认证、计费”等功能对于大部分计算机信息系统而言均可认定为“主要软件”,故可以将表格中第1项与第4项的“系统功能”作等同理解,进而认为其在“重要程度”上不具有显著差别。在控制“功能重要程度”变量的前提下,明显看到第1项的结果不法程度天然弱于第4项,这是因结果规模的隐形量级不同导致的。为统一本罪入罪的不法边界,应当“举重以明轻”,认为第1项同样包含不法结果持续时长的要求,即计算机信息系统的主要软件或者硬件不能正常运行的累计时长需达到一个小时以上,才可实现罪责刑相适应的原则。

五、结语

数据本身兼具“载体—内容”两种侧面,侧重虚拟技术与现实内容两重面向。破坏计算机信息系统罪保护“系统的正常运行”,意在保护虚拟技术面向的计算资源,而非其内数据内容的权利指涉。破坏主体的限定知悉并不意味着计算资源损毁,即系统无法正常运行,实践将侧重内容罪质的行为嫁接到本罪适用是导致适用泛化的重要原因,背后体现的是对“数据”概念不同侧面的混同与误读。因此,应当严格区分数据的不同面向,依据破坏数据不同罪质认定适用罪名。罪量标准过低也是本罪适用泛化的另一原因,虽然本文已在教义学域内提出了限制罪量标准适用的具体方法,但这一问题本质仍归根于解释条文与社会现实的脱轨,法教义学虽具解释立法机能,却终归有限。因此,超然教义理论之外,在立法中立足现实、完善规定方为解决问题的根本举措。

[参考文献]

[1][英]维克托·迈尔-舍恩伯格,肯尼斯·库克耶.大数据时代:生活、工作与思维的大变革[M].盛杨燕,周涛,译.杭州:浙江人民出版社,2013.219.

[2]高铭暄,马克昌.刑法学(第十版)[M].北京:北京大学出版社,2022.69.

[3][31]王华伟.破坏计算机信息系统罪的教义学反思与重构[J].东南大学学报(哲学社会科学版),2021(6):97.

[4][德]克劳斯·罗克辛.刑事政策与刑法体系(第二版)[M].蔡桂生,译.北京:中国人民大学出版社,2012.64.

[5][10]王莹.情节犯之情节的犯罪论体系性定位[J].法学研究,2012(2):137.144.

[6][7]王强.罪量要素:构成要素抑或处罚条件?

[J]. 法学家,2012(5):22. 24-25.
[8][12]张明楷. 刑法分则的解释原理[M]. 北京:中国人民大学出版社,2011. 473-490. 484.
[9]周光权. 论内在的客观处罚条件[J]. 法学研究,2010(6):121.
[11]张明楷."客观的超过要素"概念之提倡[J]. 法学研究,1999(3):27-28.
[13]黄荣坚. 基础刑法学[M]. 北京:中国人民大学出版社,2008. 134.
[14]柏浪涛. 规范性构成要件要素的错误类型分析[J]. 法商研究,2019(1):81.
[15][30]邢永杰. 破坏计算机信息系统罪疑难问题探析[J]. 社会科学家,2010(7):81. 83.
[16][日]伊东研祐. 法益概念史研究[M]. 秦一禾,译. 北京:中国人民大学出版社,2014. 348.
[17]李文吉. 我国刑法中管理秩序法益还原为实体性法益之提倡[J]. 河北法学,2020(5):2-19.
[18]杨猛. 法定犯证成路径之研析:以刑法教义学与刑事政策关系嬗变为切入[J]. 湘潭大学学报(哲学社会科学版),2023(1):82-84.
[19][24][29]徐春成,林腾龙. 教义学视角下破坏计算机信息系统罪的法益论辩[J]. 科技与法律(中英文),2023(4):24-27. 23-24. 23.
[20]李源粒. 破坏计算机信息系统罪"网络化"转型中的规范结构透视[J]. 法学论坛,2019(2):38.
[21]劳东燕. 个人数据的刑法保护模式[J]. 比较法研究,2020(5):45.
[22]李源粒. 网络个人数据安全刑法保护研究[J]. 重庆邮电大学学报(社会科学版),2015(6):50.
[23]王倩云. 人工智能背景下数据安全犯罪的刑法规制思路[J]. 法学论坛,2019(2):34-36.
[25]姜涛. 高空抛物罪的刑法教义学分析[J]. 江苏社会科学,2021(5):112.
[26][27]叶小琴,高彩云. 破坏计算机信息系统行为的刑法认定——基于最高人民法院第104号指导性案例的展开[J]. 法律适用,2020(14):8. 8.
[28]王爱立.《中华人民共和国刑法》条文说明、立法理由及相关规定[M]. 北京:北京大学出版社,2009. 596.

[责任编辑　何卫卫]