整治罐车运输乱象，食安监管需上“硬杠杠”

观点

针对媒体报道的“运输罐车运完煤制油后未清洗直接混运食用油事件”，7月6日，中储粮集团在其官方微博发布声明称，从7月5日开始在全系统开展专项大排查，对违反相关规定的运输单位和承运车辆依法终止运输合作。

媒体发现问题，涉事企业当日即介入，这种自我检视的态度和做法，无疑是对舆论关切的积极响应，也有利于其赢得公众信任。但要想进一步保障好食品安全，前置相关监管工作、做好预防把关是更为重要的步骤。

食品安全事关公众切身利益，其涉及的每一个环节都至关重要，这也需要相关监管的全链条跟进。对食用油而言，这就意味着，生产、运输、销售等环节上的安全把关都不可或缺。

此次引发关注的罐车运输油罐混用问题，就是在运输环节上没有做好监管把关工作。从报道看，涉事企业在运输食用油的过程中不仅没做到“专车专运”，且在罐车运完化工液体后，连最基本的清洗工作都糊弄了事，有的甚至没有清洗，这成了“行业里公开的秘密”。

这显然要求加强日常监管，督促企业持续优化安全管理机制，以更好落实食品企业的安全责任，尤其是对相关法律法规的常态化落实工作。

食品安全法明确，“贮存、运输和装卸食品的容器、工具和设备应当安全、无害，保持清洁，防止食品污染”“不得将食品与有毒、有害物品一同贮存、运输”。这也应该成为企业做好食品安全保障的法律“硬杠杠”。

中储粮此番表态及采取的措施，无疑是公众所期待的。而在专项大排查工作之后，也要通过提升相关工作的透明度，做好随时接受公众检视的准备。毕竟，食品安全至关重要，唯有各方共同发力，方能守护好公众“舌尖上的安全”。

综合自新京报等
（谚路 整理）

时代转型中非法获取计算机信息系统数据罪的适用

□ 李雁飞 荣梓童

【内容摘要】社会技术的发展和时代的转型导致非法获取计算机信息系统数据罪出现了“数据”外延泛化、手段行为趋向秘密性和非技术性、目的行为多样性以及违反国家规定要件透明化的问题，对此应当结合本罪的规范保护目的，从法教义学的角度作出契合时代的新理解。

【关键词】非法获取计算机信息系统数据罪 教义学解释 实证研究

2009年《刑法修正案（七）》为打击危害计算机网络安全的犯罪行为增设非法获取计算机信息系统数据罪，然而随着技术的发展，社会结构由现实的单一结构向现实与网络“双层社会”的结构转型，时代背景的变化导致非法获取计算机信息系统数据罪在实践中面临着新的问题，如何准确地把握和理解本罪的构成要件具有重要意义。

（一）非法获取计算机信息系统数据罪的实践样态

本项目选择中国裁判文书网数据库，以“非法获取计算机信息系统数据”为关键词进行搜索、整理，排除无效案例后共获得有效研究样本911份，从数据范围、行为方式等多个方面展开全样本研究，结果如下：

1.“数据”外延极度泛化，罪名认定争议现象严重

司法实践中对“数据”范围的认定，大概有以下四类：（1）数字化商品，即用户使用货币购买的，以电子化数据形式存在的虚拟商品或用以兑换各类虚拟产品和增值服务的产品；（2）账号密码信息，即用于确认用户在特定系统上操作权限的身份认证信息；（3）公司企业等单位系统内部所存储的基础数据信息，如游戏源代码等；（4）公司企业等单位系统内部所存储的用户个人信息，如平台注册的用户信息等。可以看到，实践对“数据”外延的理解采取了技术判断的标准，几乎囊括了一切以电子形式存在的数据类型。

2.手段行为的秘密性和非技术性趋势明显

本罪的手段行为包括以下几种：使用木马病毒等破坏性软件、利用网站既有漏洞、利用具有权限的特殊身份、利用钓鱼网站骗取、冒用他人身份以及扫号撞库。分析其年代演变可知，技术发展与法律体系的完善使得利用特殊身份等秘密且缓和的侵入方式逐渐替代了立法之初广泛存在的使用木马病毒软件等暴力破解侵入的行为。此外，以非专业人士能否实施为标准进行判断，利用特殊身份、冒用他人身份以及扫号撞库的非技术性手段行为占比高达40.6%，且从年代演变来看，技术性侵入的手段正在逐年减少，而非技术性侵入的手段则缓慢增加。

3.目的行为的多样性

刑法第285条第2款所规定的获取行为在实践中共表现有三种类型：（1）一步式取得，指获取方式与手段行为具有紧密联系性，往往表现为手段行为的附随后果，可以直接地、“一步”获取相关数据，如使用木马病毒侵入系统后自动运行获取数据，无需实施额外的操作，此类方式占全部行为的68%；（2）多步式取得，指获取行为与前手段行为间无直接联系，利用手段行为绕过系统限制后，该手段行为的作用即刻终止，获取目的的实现仍需行为人实施额外的复制、下载、传输等操作，如冒用他人身份获取数据的行为，此类方式占比37%；（3）了解取得，指通过理解、记忆的方式获取数据，属于人的脑部活动，往往只适用于部分无需或无法复制、下载、传输的数据且数据总量不大的情况，此类方式占比1%。

4.“违反国家规定”要件透明化

实践中鲜有法官在定性判断时对该要件进行分析认定，据统计，在911份有效案例中仅有6份裁判文书明确引用了前置性法律规范，占比仅有1%，这6份裁判文书所引用的前置法均是《计算机信息系统安全保护条例》（以下简称《条例》）第7条的规定，99%的案件只是简单提到“行为人的行为违反国家规定”，并没有引用具体的法律规范加以说明。因此实践中出现了“违反国家规定”要件透明化的现象，进而导致对该要件内容的理论理解匮乏。

（二）构成要件要素的法教义学阐释

1.“数据”范围的限缩理解

对构成要件的解释必须以保护法益为指导，当下本罪保护法益的理解正面临着时代转型，具体内容尚且未能形成确定结论，但“新型数据”被侵犯的客观保护需求又亟待解决，如此矛盾倒逼司法机关迫切寻求此类行为的“安身之处”，与其外观特征相符合且概念内涵本就模糊不清的“数据”自然成为了较好的“口袋”。前述数据类型虽然物理属性上具有数据的特征，但数据并非其唯一的属性，甚至不是最重要的属性，应当从规范判断的角度结合法益保护的目的导向，将以数据为载体的传统法益类型排除在外，将“数据”范围限缩解释为独立的数据类型或者数据产品。

2.技术性并非“侵入”行为的特点

手段行为缓和侵入的方式欠缺对保护系统的攻击、破解，因而对计算机信息系统本身及网络安全的侵害性较小，而对数据安全本身的威胁较大。非技术性侵入手段的高占比和上升趋势表明此类犯罪实施的门槛正在逐步降低，犯罪主体范围的扩大也使得法益面临侵害的可能性正在逐年上升。因此，对手段行为的理解应当摒弃技术性的要求，刑法285条所规定的“侵入……或者采用其他技术手段”中的“其他技术手段”并不必然修饰前述“侵入”行为，应当理解为并列关系，行为人非法使用身份认证信息获取数据库访问权限或者采用非法技术手段破解数据库访问权限的行为均属于“侵入”行为。

3.了解取得亦属于获取行为

一方面，多数案件所涉的数据体量都较为庞大，难以凭借了解的方式真正获取数据及其携带的信息；另一方面，了解属于脑部活动，不会在客观上留下证据痕迹，通过技术手段也难以得出盖然性的结论，只能凭借司法人员推断，而刑事案件证据的重要性又往往使得该种方式难以为司法机关所认可，从而导致了解取得的案例占比极少，但不可否认的是此类获取方式对某些数据体量简单但重要的信息数据而言，其对数据安全法益的侵害程度上并不会因获取手段的差异而减轻，结合本罪的规范保护目的，应当将了解取得的方式纳入刑法285条所规定的“获取”一词的范畴内。

4.“违反国家规定”要件的理解

“违反国家规定”要件并非声明性规定，其本质属于真正的构成要件要素。“违反国家规定”是对实行行为的整体性评价，但更侧重对获取（目的）行为的限定性作用，否则将会使利用合法身份访问数据库但超越授权非法获取数据的犯罪类型出罪，实践中该要件“透明化”的现象正是忽略这一认识，宏观地将其理解为“犯罪的行为违反国家规定”的结果。此外，对该要件的理解不能困于《条例》第7条的内容，党中央国务院《关于构建数据基础制度更好发挥数据要素作用的意见》明确了数据新型生产要素的地位，指出数据基础制度建设的重要作用，在此基础上，应当将《数据安全法》等侧重保护数据安全的制度内容考虑在内。