大数据时代数据犯罪的制裁思路*

于志刚　李源粒

摘　要：在大数据时代，数据成为网络的核心要素，数据范围向横向聚合与纵向深化，云计算平台成为数据挖掘的技术资源。技术变革引发刑法新的关切点，现行刑法中“数据”的范围在纵向和横向两个方面显现出时代局限性和滞后性。为解决这一问题，司法解释尝试以技术性关键词为扩张解释对象，司法实践也开始探索对数据内容的扩充。但是，由于解释观察点的错位，过于重视数据的空间性而忽略本体性，造成案件定性的困扰。大数据时代数据犯罪的制裁体系的建构，应当以数据与信息的本质差异为区分点，明确以技术资源为保护对象的内容与边界，重视多端点的数据来源和聚合性的数据应用，实现从数据到具体法益的“着陆”，明确对数据的非物权保护模式。通过严厉严密的制裁数据犯罪的罪名体系，构筑保障信息时代国家安全的法律屏障。

关键词：大数据　网络犯罪　数据犯罪　计算机犯罪　立法完善

作者于志刚，中国政法大学司法文明协同创新中心教授（北京　100088）；李源粒，德国马普外国刑法与国际刑法研究所研究人员。

“当世界开始迈向大数据时代时，社会也将经历类似的地壳运动”。① 确实，大数据时代完成了以数据为中心的一系列观念、技术、应用的技术变革，这种广泛性、根本性的变革必然将引起人类生产、交往方式的变革，社会管理方式、结构的变革，也必将呼吁与之相应的法律制度的变革。

一、大数据时代的安全问题

一般认为，大数据是指数据量巨大，通常认为数据量在10TB-1PB（1TB＝

* 本文系2012年教育部哲学社会科学重大课题攻关项目“信息时代网络法律体系的整体建构研究”（12JZD039）、中国政法大学优秀中青年教师培养支持计划资助项目阶段性成果。

① 参见维克多·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》，盛杨燕、周涛译，杭州：浙江人民出版社，2013年，第219页。

1024GB，1PB＝1024TB）以上，① 数量级应是“太字节”（2×40）的，② 并且是高速、实时数据流。③ 业界通常认为，大数据具有“4V＋1C”特征，即数据量大（volume）、多样（variety）、快速（velocity）、价值密度低（value），以及复杂度（complexity）。④ 工业和信息化部研究院《大数据白皮书（2014）》指出，大数据具有“资源、技术、应用”三个层次，大数据是新资源、新工具和新应用的综合体。⑤ 刑法需要对大数据在元数据阶段的资源性、在数据应用阶段上的现实性，以数据为对象进行关注，以区别于技术层面的数据，也区别于“旧技术”层面的数据。

大数据的核心，从存储和传输过渡为数据的挖掘和应用。在大数据环境下，数据的集中和数据量的增大给产业链中的数据安全保护带来新的威胁，数据开始成为主要的攻击对象，网络向围绕数据处理的数据网络转向。在传统的数据安全语境下，数据存储是非法侵入的最后环节，目前已形成较完善的安全防护体系。但是，在大数据应用中，如何保证数据有效利用前的安全是一个重要问题；同时，网络也面临传统攻击深化的深度威胁，随着网络节点数量的增加，安全问题也呈指数级上升。大数据包含大量用户身份信息、属性信息和行为信息，各渠道数据存在交叉检验的可能，极易造成隐私泄露威胁。大数据安全控制力度不足，会带来大数据滥用的风险。⑥ 现有的信息安全手段已经不能满足大数据时代的信息安全要求，例如，利用大数据技术的APT攻击不具备实时检测的特征，攻击代码隐藏在大量数据中，很难被发现，⑦ 黑客、间谍犯罪动机强烈，数据分析结果泄露将导致对企业甚至行业的毁灭性打击。⑧

伴随着网络向围绕数据处理的数据网络转向，数据范围在横向与纵向两个方面急剧扩张，现实生活的数字化和数据化加速，企业数据急剧聚合，规模化的数据中心出现；云计算平台形成网络资源池，数据存储和计算都利用云端资源，实现了元

① 参见耿冬旭：《“大数据”时代背景下计算机信息处理技术分析》，《网络安全技术与应用》2014年第1期。

② 参见涂子沛：《大数据：正在到来的数据革命，以及它如何改变政府、商业及我们的生活》，桂林：广西师范大学出版社，2013年，第57页。

③ 参见马建光、姜巍：《大数据的概念、特征及其应用》，《国防科技》2013年第2期；王倩、朱宏峰、刘天华：《大数据安全的现状与发展》，《计算机与网络》2013年第16期。

④ 参见刘鹏、吴兆峰、胡谷雨：《大数据——正在发生的深刻变革》，《中兴通讯技术》2013年第4期。

⑤ 参见工业和信息化部研究院：《大数据白皮书（2014）》，第1—2页。

⑥ 参见张尼、张云勇、胡坤等编著：《大数据安全：技术与应用》，北京：人民邮电出版社，2014年，第62—72页。

⑦ 参见王文超、石海明、曾华峰：《刍议大数据时代的国家信息安全》，《国防科技》2013年第2期。

⑧ 参见亓冬、吴洋、彭默馨：《直面大数据对信息安全的挑战》，《保密工作》2012年第8期。

数据向有意义信息的转化，使数据的价值处于动态增生之中。以此为背景，大数据时代数据犯罪的指向，不再仅仅是对于计算机信息系统中存储、处理、传输数据的增加、修改、删除和干扰，而是演变为以大数据对象为中心，纵向侵害技术与现实双层法益，形成的一个多行为方式，危害后果横向跨越个人、社会、国家各层面与政治、军事、财产、人身和民主权利各领域的大犯罪体系。具体地讲，大数据时代的数据犯罪，是指以大数据即以数字化形式进行技术处理的一切数据为犯罪对象的犯罪，包括以账户、访问控制数据为核心，并发散至电子痕迹、生活行为、城市管理等各种非结构化数据，以及从计算机数据延伸到物联网、智能手机、可穿戴设备等多终端数据的犯罪。犯罪的行为方式，不仅体现为技术破坏、非法获取的行为，也体现为大规模数据监听、监控、窃取、过度挖掘、恶意滥用等一系列行为；犯罪的危害后果，除了破坏计算机信息系统功能，还危害个人的财产安全、隐私、人身、人格安全，严重的则危害经济秩序、国防利益与国家安全。数据犯罪给现行刑事立法和司法提出了前所未有的挑战，面对日益猖獗和直接威胁国家安全、公共安全的数据犯罪，刑法的制裁能力和打击半径力有不逮，在国家整体安全战略和现实罪情需要面前已经滞后。

二、刑法中“数据”概念的时代局限性和滞后性

现行刑法对计算机信息系统计算能力和技术资源的保护，是静态的、非在线的。而大数据是围绕数据动态处理模式的革新，作为对象的数据的范围发生了巨大变化，这种技术范式的转变，必然要求刑法层面相应的范式转变。具体来说，计算能力的技术资源保护和体现为信息的数据对象的保护，都需要刑法跟进，而现行刑事立法和司法解释都还局限在数据范围这一表象的条文规范和扩张解释之上，具有时代局限性和滞后性。

（一）现有数据范围的局限

在现行刑法中，数据是指计算机信息系统数据，这一概念相对于大数据时代数据的量级与结构来说过于狭隘且滞后，导致许多现实中出现的具有现实危害的数据窃取行为无法纳入刑法评价范围之内。

1. 刑法分则的“数据”：外延狭窄、内涵滞后

数据作为一个技术名词，在现行刑法和司法解释中没有明确解释。从直观上看，数据犯罪是《刑法》第 286 条规定的非法获取计算机信息系统数据罪，置于《刑法》分则第六章妨害社会管理秩序罪第一节，属于扰乱社会秩序犯罪，为 2009 年 2 月 28 日《刑法修正案（七）》第 9 条所增设。非法获取计算机信息系统数据罪，是指违法国家规定，侵入国家事务、国防建设、尖端科学技术领域以外的计算机信息系

统或者采用其他技术手段，获取该计算机信息系统中存储、处理、传输的数据，情节严重的行为。① 计算机信息系统中存储、处理或者传输的数据，是指在计算机信息系统中实际处理的一切文字、符号、声音、图像等内容有意义的组合。② 作为此罪犯罪对象的数据，是作为计算机信息系统功能实现的载体，被限定在计算机信息系统范围之内，更多地是指信息系统容器内部的静态数据库安全。信息系统中的数字信息的安全，在很多情况下就是指数据库中产生和保存的数据，③ 包括数据库的完整性、可信性、系统灵活性、用户方便性、篡改检测等。④ 从阶段上看，进入信息系统内部，为信息系统的功能实现而存储、处理和传输的内部数据，才是刑法条文所保护的对象。更广泛的数据来源和更多样杂乱的数据结构，只要未存储到系统内部，未按照系统的组织目标进行规整和排列，都被排除在刑法的保护范围之外。

如果考虑到对数据内容和形式的要求，刑法分则中“非法获取计算机信息数据罪”的对象范围，实际上还要窄于此处所称“数据库数据”的范围。2008 年，在第十一届全国人大常委会第六次会议上，全国人大法律委员会在论证非法获取计算机信息系统数据行为应当追究刑事责任时阐述，“一些不法分子利用技术手段非法侵入上述规定以外的计算机信息系统，窃取他人账号、密码等信息……严重危及网络安全。”⑤ 此外，2011 年两高《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《计算机安全解释》）对《刑法》第 285 条第 2 款的“情节严重”作了进一步解释，其中对于数据的类型规定比较单一。该解释第 1 条规定，非法获取计算机信息系统的数据，“情节严重”的情形包括，获取支付结算、证券交易、期货交易等网络金融服务的身份认证信息 10 组以上的，或者这以外的身份认证信息 500 组以上的。据此，数据类型是指身份认证信息。该解释第 11 条规定，身份认证信息是指用于确认用户在计算机信息系统上操作权限的数据，包括账号、口令、密码、数字证书等。基于以上文件可以发现，从立法理由和司法解释两个层面，关注的都是数据库中比较狭隘的认证信息，即具有一定权限识别意义的数据。因此，《刑法》第 285 条第 2 款所保护的数据，是限于计算机信息系统内部的、侧重于信息系统自身功能维护的、以访问控制为主要考虑的数据。此种数据类型过于附着于信息系统功能，没有关注数据自身内容属性上的价值与保护必要，而且类型单

① 参见高铭暄、马克昌主编：《刑法学》，北京：北京大学出版社，2011 年，第 536 页。

② 参见陈兴良：《规范刑法学》，北京：中国人民大学出版社，2008 年，第 814 页。

③ 参见陆宝华、王楠主编：《信息系统：安全原理与应用》，北京：清华大学出版社，2007 年，第 324 页。

④ 参见陆宝华、王楠主编：《信息系统：安全原理与应用》，第 329 页。

⑤ 《全国人民代表大会法律委员会关于〈中华人民共和国刑法修正案（七）（草案）〉修改情况的汇报——2008 年 12 月 22 日在第十一届全国人民代表大会常务委员会第六次会议上》，《全国人民代表大会常务委员会公报》2009 年第 2 期。

一、范围狭窄，局限于以验证为内容的数据。

2. 现实中数据的外延复杂多样

静态数据库与特定类型的结构化数据，是计算机信息系统时代的数据概念。大数据时代的数据概念，在纵向上由技术运算深入到生活细微，在横向上由特定测量性数据发展为全面的记录型数据。这两方面的变化都对原有刑法分则中“计算机信息系统数据”概念提出了实质性挑战。

从纵向上看，数据窃取的端点分散，同时这些端点日趋生活化，深入到个人的日常活动中。与传统的电脑网站平台相比，移动互联网中的手持终端设备更加私密、也更及时和不安全。用户的数据在移动互联网环境下更容易关联个人的关键行为活动，也更容易展示个人社会联系，例如，短信记录、通话记录、位置信息，等等。中国互联网络信息中心在《2013 年中国网民信息安全状况研究报告》中的统计数据表明，与 2012 年相比，网民遇到手机垃圾短信和骚扰电话、中病毒或木马、账号或密码被盗的比例都有较大幅度下降，而手机恶意软件和个人信息泄露的比例增幅分列前两位。① 可见，在移动网络中，重要数据泄露的威胁已经开始由账号密码等个人信息泄露，转向范围更广泛的用户跟踪，即更广泛的行为数据的窃取。

从横向上看，大规模的数据中心也成为重要的数据泄露渠道，并且受害人数众多，数据信息量丰富。在企业大规模的数据泄露事件中，被窃取的用户数据数量巨大。由于企业对用户数据进行了全面记录，用户数据包含了身份、隐私、行为数据、财产以及交易数据等。这些数据完全超出虚拟空间和技术层面，直接关系到生活的各个方面。2014 年 3 月 22 日，乌云漏洞平台发布消息称，携程网用户支付信息出现漏洞，漏洞泄露的信息包括用户的姓名、身份证号码、银行卡卡号、银行卡 CVV 码以及银行卡六位 Bin，等等。②

3. 现实中数据的内涵具有独立性

在大数据时代，数据已经与技术运算成为不同的独立对象，并且从阶段、范围上都无法形成固定的对应关系。大数据对传统技术性数据概念的挑战集中于两点：一是宏观上，大数据与计算逐步分离，成为不同的层次和阶段；同时，网络的定义极大扩张，更加抽象化和智能化，成为“天上飘着的云”，并带来质的变化。云端的意义在于数据的集成化应用，通过对非结构数据的分析和应用改变生活、控制生活，由网络的联结作用和信息传输作用跃升为后续的整合作用，数据的重要价值内涵在系统存储环节之前就在记录现实的元数据阶段潜在存在，并通过应用阶段对接现实。二是微观上，大数据向终端深入，而这些终端的物化特征明显。与主体个人身份和

① 中国互联网络信息中心：《2013 年中国网民信息安全状况研究报告》，第 11 页。

② 参见张司南：《从 XP“裸奔”到支付宝漏洞 国内信息安全挑战层层加码》，2014 年 6 月 30 日，http://finance.chinanews.com/it/2014/06-30/6331029.shtml，2014 年 9 月 1 日。

日常生活相关的数据成为数据价值的主要内容，而终端计算能力明显弱化，存储、处理、传输都不是针对数据的主要技术过程，仅是获取便已足够。

目前，新的数据类型的问题已开始发生。2011 年 6 月起铁路实行实名购票制，二维码信息作为车站检票的主要途径，尚无防破解的技术，经扫码软件解码后，就可轻易获取个人身份信息和订票手机、电话等信息。① 2012 年 4 月，英国《经济学人》刊文认为，3D 打印技术将与其他数字化生产模式一起，推动第三次工业革命的实现。3D 打印是将计算机设计出的物体分解成若干层平面数据，将多维制造变为简单的由下至上的二维叠加。② 第三次工业革命将借助于发达的信息、通信手段以及网络平台，突破传统产业的地理局限，形成网络意义上的集聚，即产业集群发展的虚拟化。③ 网络由现实产业的传输层面逐渐向实体层面过渡；网络数据由计算机信息系统的技术传输对象逐渐变成了现实性载体，对信息系统技术性无重要意义的数据，可能是大数据时代的重要刑法关注对象。

同样的“0”和“1”的数据符号，由一维到二维、三维的发展，带来的是数据本身的独立性意义。从某种意义上说，数据本身就含有所指客观事物的关键信息，根本无需借助于联网、计算、存储、处理和传输等技术过程。数据本身包含的这种价值，与其说体现为技术层面，不如说体现在其与现实世界受保护法益的联系上。这样的数据，从价值内涵上无法在技术层面上合理界定，更无法为现有刑法所保护的技术属性的数据概念所涵摄。因此，从行为规范的意义上理解数据，是大数据时代的必然要求。

（二）司法层面的应对举措

司法解释敏锐地观察到实践中技术迭代带来的新问题，对计算机信息系统等技术关键词进行了扩张解释；在审判环节，已经有判例扩张数据的范围，应对现实中的问题。

目前，司法实践的解决思路是扩张解释“计算机信息系统”这一技术概念。《计算机安全解释》第 11 条规定：本解释所称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。这里首次使用“计算机系统”的术语，以弱化“计算机信息系统”的性能特征。这一解释打破了对于传统计算机的固化解释，将几乎所有与计算机相关联的网络终端

① 参见孙峰、徐忠：《“二维码”可能成新型犯罪工具》，2014 年 3 月 21 日，http://www.cpd.com.cn/n12550435/n21884632/n21884660/n21884689/c22143371/content.html，2014 年 6 月 19 日。

② 参见蒋建科、李秋荣、杭慧喆：《一项颠覆性的制造技术正在进入普通人的生活——3D 打印第三次工业革命的重大标志》，《人民日报》2013 年 1 月 4 日，第 20 版。

③ 参见孙柏林：《试析“3D 打印技术”的优点与局限》，《自动化技术与应用》2013 年第 6 期。

设备，无论屏幕大小，包括手机、平板电脑、家用智能电器等都扩张解释为计算机信息系统，而无需判断犯罪对象是否属于计算机。① 从技术上来说，这样的扩张没有问题，但是面临大数据的技术冲击，寻求更贴切的解决路径仍须从长计议。

《计算机安全解释》对一个并列短语“计算机信息系统和计算机系统”作了从实质功能上认定的扩张解释，实际认识且承认计算机信息系统与计算机系统之间的区别，即到网络应用层与到更底层计算机结构之间的区别；同时刻意强调对二者的趋同对待，仅聚焦于计算机的数据自动处理功能与数据传输功能，不强调对以功能和业务应用为前提，对后续罗列的各个组成部分没有完整性和体系性的要求。由此可见，司法解释是以对“计算机信息系统”这一技术名词的解释为核心，通过对其不断扩张，以适应互联网发展趋势，使信息系统与网络逐渐融为一体。因此，司法解释的扩张思路是：形式上围绕技术关键词，且事实上仅针对“计算机信息系统”这一关键词进行解释；实质上将网络作为考量的主要因素、以扩张系统适应网络特征为解释目的。

但是，司法解释一直没有对“数据”这一技术概念作出解释。在实践中，已经发生大规模窃取具有重要意义的身份认证信息之外的系统数据的犯罪活动，部分行为已经在司法实践中被认定为属于非法获取计算机信息系统数据罪中的“数据”，因此，“数据”的范围实际上得以扩充。在北大法律信息检索系统中，检索以“非法获取计算机信息系统数据罪”为罪名定罪处罚的刑事案件，共 31 起，另外有 5 起窃取计算机信息系统内游戏账号、秘密数据的案件以盗窃罪定罪处罚，1 起盗窃电信公司系统内手机号码案件以破坏计算机信息系统罪定罪处罚。上述案件中作为犯罪对象的“数据”的范围，包括信用卡资料、游戏账号等身份认证信息，同时也出现了值得关注的新动向。在乐某某、王某非法获取计算机信息系统数据案中，被告人所获取的数据就不是特定的身份认证信息，而是药品用量信息。② 药品用量统计数据虽然也是计算机数据记录，但已超出计算机信息系统完整性，凸显了大数据时代计算机数据的多样化、记录性特征；而其所指的“数据”，从内容上已经不再局限于账号、密码、身份认证信息等权限型的信息。可见，司法实践中对数据的理解，已经开始关注其现实意义，而不仅仅将其看做计算机信息系统的运算和管理对象。

（三）解释思路的问题

司法解释从网络的角度进行技术性概念的解释，意在顺应互联网发展的科学潮流，但是，在刑事层面的回应存在不够深入和准确的问题。司法层面的应对是基于

① 参见于志刚：《“三网融合”视野下刑事立法的调整方向》，《法学论坛》2012 年第 4 期。

② 上海市黄浦区人民法院（2014）黄浦刑初字第 106 号判决书，上海市第二中级人民法院（2014）沪二中刑终字第 229 号判决书。

现实的数据范围的困扰而生，也仅停留于数据外延扩张的表层，没有探求数据的内涵本质和数据与计算资源的分别。尤其是解释的重点偏重于网络的空间特征而没有落脚于数据的本体之上，造成已有扩张解释在理论和实践层面都存在一些问题。

1．观察角度问题：观察点错位

司法解释仅在信息系统的技术概念上进行较大扩张，而没有对数据的概念予以调整，表达了这样一个逻辑："信息系统"的概念扩张自然而然地等同于"数据"的范围扩张，因此无需再解释"数据"这一附属概念。此种逻辑局限于早期对"计算机犯罪"的认识，存在一定的滞后性。

数据的范围最初与计算机信息系统的边界是一致的，"计算机信息系统内存储、处理、传输的数据"描述了需要保护的数据范围。但是，网络因素扩展了"传输"这一环节的数据，并使"信息系统"的技术概念向"网络"的传播概念逐步松动。犯罪对象的"网络"在不断扩大，从计算机信息系统到计算机网络，推动了刑法视野中网络犯罪从"计算机犯罪"到"网络犯罪"的称谓过渡和内容合一。① 网络因素的介入，实现了计算机信息系统数据蔓延到联网的所有终端，融合了广泛的网络数据。《计算机安全解释》的问题，在于没有能够明确区分"计算资源"与作为计算资源对象的"数据"二者的区别。在大数据时代，沿用以信息系统限定数据的思维，就只能将计算机信息系统的概念无限扩张，并进一步淡化其技术特征，以致宽泛到几乎有数字化特征的终端都被纳入一个庞大的系统，结果就是系统概念的虚无化。

2．切入侧面问题：重视空间性忽略本体性

司法解释回应了由系统到网络的信息传播方式变革，但对这一变革的认识却停留在空间的层面而没有深入本体层面。司法解释从信息系统的概念出发，进行系统边界扩张，试图将网络包容在内。但是无论信息系统或者网络，都是作为信息处理、传播的载体和平台，空间上的演变离不开最终数据或信息的本体性。为了更好地应对网络因素导致的犯罪滋生、法律规制不力的现实问题，司法解释选择了以技术性关键词为核心的思路。表面上是重新界定计算机信息系统和计算机系统的计算能力标准，但实际上是以网络涵盖范围为主要考虑因素。网络的本质在于将分散的终端联结起来，并实现即时、超地域、便捷无阻的信息交互和汇聚，最终的功能是传播信息。网络因素的意义在于改变了信息传播的方式、范围、效率，但并未改变信息本身，也没有改变物质、能量等最基本的本体性概念。无论是刑事法律的废、改、立，还是司法层面的扩张解释，都要针对具体的犯罪对象、行为、后果、责任等概念和理论进行，网络是一个影响因素和分析变量，在研究过程中属于视角和理念，而不是对象本身。尤其是对计算机信息系统这样的犯罪对象进行解释，更不应将网络直接融入对象的解释之中。

① 参见于志刚：《网络犯罪的发展轨迹与刑法分则的转型路径》，《法商研究》2014 年第 4 期。

3．方向问题：向上位概念扩张

计算机犯罪的犯罪类型可分为三类，一是对侵犯技术资源、计算能力的犯罪，二是对数据的非法获取，三是非法利用数据、技术手段进行的其他多种法益的侵害行为。这三种维度的问题在网络这一上位概念中交织存在。因此，如果过于向上位概念扩张，会造成几种现象之间界定不清，无法有针对性地对违法犯罪行为进行有效打击，也无法准确地对相关法益进行必要保护。

在信息时代，人们的生活离不开网络，“几乎所有的犯罪都可以称之为网络犯罪”。如果对技术性概念的解释向网络这一几乎无所不包的上位概念“逃逸”，会导致刑法的法益保护指向性不明，行为规范不清晰，刑罚的否定评价没有针对性，传达功能不能很好地实现。

4．实际影响：案件定性的困扰

从解释后的信息系统概念看，《刑法》第 285、286 条对针对计算机信息系统犯罪行为的制裁，是作为妨害社会管理秩序犯罪定性的。计算机信息系统的安全秩序作为需要刑事保护的秩序，仅以单点化的具有简单数据处理功能的智能终端予以论证或者解释略显薄弱。信息系统的社会重要性的评判，需要依据其受到破坏的影响情况进行安全等级赋值。根据《信息系统安全保护等级定级指南》，赋值因素包括业务数据、服务范围、业务处理等因素。① 各个被组织起来的各终端的独立数据处理自动功能并不能反映信息系统的核心特征，也无法体现刑法通过分则罪名设置所希冀保护的重要法益。

司法解释的扩张实际上在网络犯罪阶段已经显现出来一定的实践层面问题。抹去了计算机信息系统的功能性特征，就会将信息系统概念扩张到网络范围，并且无法区分信息系统与普通入网端口。技术性的淡化会导致“以网络为对象的犯罪”和“利用网络实施的犯罪”界限难以划分。司法实践中出现了《刑法》第 286 条沦为“口袋罪”的现象，即将“计算机信息系统功能”扩张解释为“计算机信息系统数据”，进而，再将数据一词的外延由“数据库中的数据”扩展到“一切数据”。② 大数据时代如果不区分数据和技术资源，这样的概念替换和混淆必将会愈演愈烈。

三、大数据时代数据犯罪的特点和趋势

计算机通过对数据的自动化处理改变了人类的生产、生活方式，而到了大数据时代，数据的意义已经超越计算能力层面，其本身已成为重要的政治、经济资

① 参见陆宝华、王楠主编：《信息系统：安全原理与应用》，第 424—425 页。

② 参见于志刚：《网络犯罪的代际演变与刑事立法、理论之回应》，《青海社会科学》2014 年第 2 期。

源。在这一背景下，数据犯罪的关注点不仅是虚拟的技术层面和计算阶段，而是向现实的法益靠拢，并体现为元数据的分散端点和数据应用中的聚合中心的结构。刑法原有的针对数据犯罪的制裁体系，需要针对这些现实特征作出调整和回应，除关注数据对象的界定外，还需关注数据犯罪后果的现实化、多维化，实现与刑法体系的衔接。

（一）数据窃取独立的现实危害性

在计算机犯罪形成的早期，黑客行为主要以个人炫耀技术为动机。电子商务兴起后，挑战、攻击系统的网络犯罪快速消减，利用网络为工具的传统犯罪爆发式增长，利用计算机实施的财产犯罪占绝大多数。① 大数据时代，出现了专业的数据中间商②和数据中间人。③ “一些不法分子通过非法窃取海量个人信息，打包出售给信息中介企业和个人，转手再贩卖给企业或网络犯罪团体等，挖掘被人们忽略的信息成为了他们获取高额利益的利器。”④ 数据财富的巨大诱惑，使得这一行动具有聚集性和集团化的趋势，这些犯罪行为被系统化、产业化，使得数据安全威胁更具针对性和多样性。⑤

（二）数据犯罪的宏观趋势

大数据时代，数据窃取的新趋势是非特定的风险和无序开始显现。基于“一云多端”的数据来源和数据运算结构，以及大型企业数据中心汇集分散终端数据的数据幂律分布结构，数据窃取从计算过程，逐渐转移到云端之下的各种生活化硬件化终端的个人数据和云端之上针对海量用户聚合数据的窃取，云计算本身成为数据价值实现的关键挖掘环节。

所谓风险，是从阶段上判断的。网络相当于围绕数据处理运转的系统，元数据阶段价值密度低，但“大数据的核心就是挖掘出庞大数据库独有的价值”。⑥ 造成这些变革的信息技术属于整体技术的一部分，因而具有 20、21 世纪一般技术风险的

---

① 参见于志刚：《网络犯罪的代际演变与刑事立法、理论之回应》，《青海社会科学》2014 年第 2 期。

② 例如，订票系统 ITA Software 将数据提供给预测机票价格的 Farecast。

③ 例如，Quantas 在通过帮助网页记录浏览历史的过程中开发了线上系统，记录用户数据以更有针对性地发送广告。

④ 参见蔡晓卿：《二维码成网络诈骗新渠道　大数据时代安全问题凸显》，《通信信息报》2014 年 1 月 22 日，第 A05 版。

⑤ 参见《暴利构筑黑色产业链　数据安全如何脱困》，2013 年 5 月 1 日，http://sec.chinabyte.com/180/12605180.shtml，2014 年 6 月 16 日。

⑥ 参见维克多·迈尔-舍恩伯格、肯尼斯·库克耶：《大数据时代》，第 102 页。

特征，20 世纪 80 年代以来，这些变革则在“风险社会”理论予以讨论。① 大数据时代的风险，表现在云计算对于低价值密度的数据进行挖掘的信息价值实现过程，使元数据窃取的也具有核心信息泄露的不确定性。所谓无序，是从结构上判断的，“幂律最突出的特征不是有很多小事件，而是大量微小事件和少数非常重大的事件并存”。② 这种规律体现为，移动互联网智能终端的微小数据犯罪受害者众多，而针对大型企业的用户数据窃取则会使数据窃取事件的受害人提升至百万级别。

风险和无序这两种趋势，体现了大数据时代数据窃取无尺度、聚团性的复杂结构。这就是传统刑法无法应对大数据复杂性的原因，传统刑法面对的是常见的系统，这样的系统中量仍然遵循钟形曲线，因而刑法制度过于单一和特定化。

（三）数据犯罪危害后果的多重性

大数据时代，数据的重要性空前凸显，围绕数据本质、地位、特征的研究，是思考刑法体系对数据相关犯罪正确回应的前提，从数据生命周期的应用阶段理解数据价值及数据犯罪的社会危害性，是刑法体系实现有效打击的关键。

在大数据时代，虚拟的计算机处理的数据与信息具有深切关联性。信息时代的数据统指一切保存在电脑中的信息，包括文本、图片、视频等，也是信息的代名词，范畴比信息还要大。③ 数据无限接近纪录的趋势表明，数据即现实生活在计算机虚拟空间中反映的大数据价值在于潜藏在数据背后的价值，“主要是通过数据的整合、分析和开放而获得”，④ 即借助网络技术资源获得。利用网络对海量信息的强大汇聚和分析能力实现大数据应用，数据犯罪的后果直接体现在现实层面。例如，在军事领域，数据窃密直接威胁国防利益和国家军事安全。由于信息流在战争中的作用越来越大，信息化战争中决定胜负的关键因素已不是消灭敌人有生力量的多少，而是能否首先抢占制信息权。⑤ 据预计，政府、电信、银行将是最先使用大数据工具的行业。⑥ 因此，数据的应用阶段同样关乎社会秩序和公共安全。数据和信息的关联表明，大数据时代的数据犯罪问题的刑法回应，除了在技术层面对数据进行保护外，

① 参见乌尔里希·齐白：《全球风险社会与信息社会中的刑法：二十一世纪刑法模式的转换》，周遵友、江溯等译，北京：中国法制出版社，2012 年，第 288 页。

② 参见艾伯特-拉斯洛·巴拉巴西：《链接：商业、科学与生活的新思维》，沈华伟译，杭州：浙江人民出版社，2013 年，第 100 页。

③ 参见涂子沛：《数据之巅》，北京：中信出版社，2014 年，第 256、257 页。

④ 参见涂子沛：《数据之巅》，第 258 页。

⑤ 孙峥皓、汪宏昇、阎岩、岑小锋、邓志均：《浅谈信息化战争对大数据存储与分析的要求及对策》，2013 第一届中国指挥控制大会论文，北京，2013 年 8 月，第 677 页。

⑥ 钟瑛、张恒山：《大数据的缘起、冲击及其应对》，《现代传播》2013 年第 7 期。

更应寻求刑法体系的完善予以合理应对。刑法需要以更深刻的眼光解决技术层面的困扰，真正关注到技术背后公民、社会和国家存在状态的法益。

四、大数据时代数据犯罪制裁思路和罪名体系建构

以现行刑法的固有框架为依据和背景，思考大数据时代数据犯罪的制裁思路，在此基础上建立有效制裁数据犯罪的罪名体系，是当务之急。

（一）数据犯罪核心罪名体系构建

在大数据时代，针对数据处理的动态系统，应当更加明确和精细地区分不同保护对象，针对不同数据处理阶段，各有侧重地实现恰当与必要的刑法条文设置。

1．明确以技术资源为保护对象的内容与边界

《刑法》第285、286条是对于计算机信息系统资源的保护，即对计算机信息系统功能的维护。计算机信息系统功能，是指在计算机中，按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索的功能。①

《刑法》第285条第3款已经体现了对网络化的计算能力和计算资源的保护。非法控制计算机信息系统罪主要是针对僵尸网络的现象。僵尸网络最大的危害在于对网络流量的大量吞噬，② 技术性服务只是僵尸网络的派生利益，该派生利益正是源于僵尸网络对网络资源的非法占有和使用。③ 这其实是滞后的“计算机信息系统”概念在面对互联网技术发展冲击时应当采取的正确切入点，即集中于互联网的技术变革，对原有的技术资源保护对象作出扩张解释。

在大数据时代，信息系统的功能性体现为更动态化和个性化的以服务导向的云端技术系统架构，计算机运算已经由信息系统转变到云资源池，这样的计算平台显然依托于网络，并以计算能力和计算资源为其价值。如果说在计算机信息系统时代，计算能力和数据还是一个依照功能、原则、目标紧密组织起来的整体，那么在大数据时代，纯粹的网络犯罪实质上必然是基于对网络资源的侵害，是对计算能力和服务能力的侵害，这种处理和运算能力本质上是一种能量。传统刑法对纯粹的、传统的计算机犯罪的制裁，意在对信息系统功能的完整性、可靠性、安全性进行保护；经历互联网的发展，刑事立法开始逐步转向对网络资源的保护；到了大数据时代，则应侧重保护资源层的云计算资源。

因此，对技术性关键词的解释需考虑网络因素，这应集中体现为对网络资源的

① 参见陈兴良：《规范刑法学》，第814页。

② 参见于志刚：《传统犯罪的网络异化研究》，北京：中国检察出版社，2010年，第183页。

③ 参见于志刚：《传统犯罪的网络异化研究》，第188页。

重视。换句话说，对数据的广泛来源、数量庞大和现实控制力所带来的刑法问题，无法以技术层面的扩张解释一并解决，必须回到数据本身进行探索。

2. 增设以网络数据为独立犯罪对象的罪名

欧盟和德国的立法体现了直接保护数据的思路。欧洲理事会《网络犯罪公约》第 4 条规定了数据干扰行为，即故意实施无权限的对计算机数据毁损、删除、破坏、变更或者干扰的行为。这与公约第 1 条“非法存取”行为、第 5 条“系统干扰”行为是分别规定的，是以数据为犯罪对象的单独立法。《德国刑法典》第 202a 条“数据窃探”行为，即未经授权非法为自己或他人窃探经特别保护的数据的行为，也是针对数据的立法。可见，数据独立作为刑法分则的保护对象，是一种经过检验的立法思路。

我国刑法分则以数据为对象的罪名，是第 285 条第 2 款“非法获取计算机信息系统数据罪”。这一罪名在增设时已考虑到数据的重要性，与针对系统资源进行侵害的侵入、非法控制和破坏等行为方式作了区分。但是，由于对非法获取的行为界定为“非法侵入计算机信息系统或其他技术手段”，对数据界定为“计算机信息系统中存储、处理和传输的数据”，因此，对数据作为保护对象的独立性仍然较弱，没有针对不同技术对象予以区别保护。

事实上，计算资源的保护是对能量的保护，仍然可以延续传统刑法对于物权的保护模式，通过使用盗窃等财产权不同层面的价值分析予以合理评价。但是数据（一般数据，非病毒等针对计算机信息系统功能进行破坏的有害数据）是可能转换为有价值信息的数字化符号的，虽然需要以电磁等能量完成记录，也需要记录于一定的物质载体（如硬盘、磁盘）之上，但是，它的价值都不体现在这些与之相关的能量或物质上，而是体现在其自身的内容上。因此，应当采取单独的保护思路以正确评价数据作为对象的法益价值，对于数据窃取行为作出正确的刑法评价。

刑法需要以行为规范创设一般人的行动预期状态，设定行为规范以保护法益。[①] 在现阶段，可以采取温和的过渡方式。针对行为手段“软化”的窃密行为，例如，网络窃听窃取大量元数据，或者非以计算机信息系统为攻击对象或攻击载体的情况，如物联网、移动互联网智能终端等作为网络接入的情况，仍以原有的非法获取计算机信息系统数据罪来处理。长远来看，可以考虑彻底转向以数据为中心的罪名设置思路，并在分则罪名体系中体现；更进一步，也可制定保护数据资料的单行立法。对数据资料的保护，不适用以保护财产权利或者保护作为计算资源能量的物权保护模式，需要制定更系统和细致的、针对信息的行为规范。

3. 重视对多端点的数据来源和聚合性数据应用的保护

① 参见高桥则夫：《规范论和刑法解释论》，戴波、李世阳译，北京：中国人民大学出版社，2011 年，第 7 页。

从大数据发展状况和数据犯罪的宏观趋势看，未来数据保护立法应侧重于对个人数据和企业数据中心的保护。对个人数据的保护已经引起立法重视。1995年，欧盟通过了个人数据保护指令，2002年和2006年又针对电信领域的通讯数据颁布了更细致的数据保护指令。然而，个人数据保护的问题在欧盟一直争议颇多。2012年1月25日，欧盟委员会提出全面改革1995年数据保护指令的建议，以增强对个人数据的保护，① 应对全球化和科技发展的挑站，例如社交网站、云计算、位置服务和智能芯片。② 我国《刑法修正案（七）》增设第253条之一，出售、非法提供公民个人信息罪和非法获取公民个人信息罪。

与此相对的是，企业大规模汇聚用户数据，数据中心的规模、数据中心持有的数据内容、数据覆盖维度、数据敏感度，目前都急需法律关注和保护。大数据加剧了网络数据与数据主体的分离，如身份、交易数据、行为、位置数据等在空间上脱离主体，而集中于提供网络资源和网络服务的中间方。欧盟最新的个人数据保护立法改革关注到此类需求，通过相关变更体现了对数据管理者、处理者和共同管理者责任义务的加重，以更好地进行风险分担。③ 一是根据云计算等更复杂的数据在线存储环境，规定了更详细的责任分配规则，增加共同管理者的主体并规定连带责任；二是对违背指示的处理者视为管理者，对实质上管理控制数据的处理者扩张其责任；三是在责任分配机制中，增加处理者的损害赔偿责任，同时规定共同管理者或者参与数据处理的多重处理者的连带责任。④

（二）由数据到具体法益的“着陆”

一直以来被忽略的数据，应当以其信息价值为依据，完善整个关于数据的独立保护体系；通过对信息内涵的解释、细化和入罪情节的合理设置，寻求对数据的完善的刑法保护体系。

1. 刑法非物权模式保护体系的完整化

根据法益不同，我国现行《刑法》制裁的信息犯罪分别置于相关章节，主要包括第253条出售、非法提供公民个人信息罪、非法获取公民个人信息罪，第219条

① “Commission Proposes a Comprehensive Reform of the Data Protection Rules,” 2012年1月25日，http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm，2014年7月1日。

② “Why Do We Need an EU Data Protection Reform?” http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/1_en.pdf，2014年7月1日。

③ Article22，23，24，26，27，30，COM（2012）11 final.

④ Nina Gumzej，“Data Protection for the Digital Age：Comprehensive Effects of the Evolving Law of Accountability,” *Juridical Tribune*，vol. 2，no. 2（December 2012），p. 84.

侵犯商业秘密罪；还包括关于保护国家秘密和情报的条文，即第111条为境外窃取、刺探、收买、非法提供国家秘密、情报罪；第282条第1款非法获取国家秘密罪，第282条非法持有国家绝密、机密文件、资料、物品罪；第398条故意泄露国家秘密罪、过失泄露国家秘密罪；第431条第1款非法获取军事秘密罪、第2款为境外窃取、刺探、收买、非法提供军事秘密罪；第432条故意泄露军事秘密罪、过失泄露军事秘密罪。这些罪名涉及的犯罪对象包括：公民个人信息，商业秘密，国家秘密、机密、绝密，情报，军事秘密。现有刑法分则关于信息的保护条文，基本上覆盖了各类重要法益，从政治、军事、经济和个人权利等层面，将情报间谍、军事间谍、商业间谍和隐私间谍等违法行为纳入刑法制裁体系之中。然而，在工业时代贴切合体的刑法分则用语，在大数据时代难免存在内容价值对等、反映形式非结构化的新问题。有必要对刑法分则的关键词进行调整，以包括直接体现刑法所关注的重要法益的数据。

数据与信息有多种表现形式，但核心内容是同构的。对刑法所保护的重要法益价值，信息的重要性体现在其内容上，数据的意义则体现在对数据对象的反映上，当数据的反映同质于信息的内容时，单纯技术角度定义的数据便具有了现实意义。“对违法构成要件的解释结论，必须使符合这种违法构成要件的行为确实侵犯了刑法规定该犯罪所要保护的法益”。① 信息是已经直接反映有价讯息、情况和状态的描述，而数据可能只是具有信息价值可能性的符号、图形或字母，经过对比和挖掘，这些数据可以产生重要信息，因此具有保护必要。从信息的角度分析和理解数据，实际上是对具有刑法意义的法益予以更充分和全面的保护，而对刑法分则中原有的信息类语词，也应作相应扩大和动态的解释。

我国《刑法》第253条非法获取公民个人信息罪中“公民个人信息”的界定，应当认为，即便只是个人的非敏感信息，但这些针对特定主体、有明确目的收集的信息，实际上与家庭地址、电话号码等敏感信息具有同样重要的价值。小数据②甚至比传统的个人档案还要详细，它从睡眠、饮食、出行、作息等方面事无巨细地记录了一个人，如果用于诈骗、敲诈勒索、绑架、盗窃等犯罪，会带来巨大危害。所以，个人信息的范围虽然限定为个人核心信息，但是，有针对性和特定性的个性化数据记录完全能够实现从一般数据到个人核心信息的转化。

通过对“公民个人信息”、“商业秘密”、“国家秘密、机密、绝密”、“情报”、“军事秘密”等信息的解释，不仅关注到数据的价值可能性，提前了刑法的保护阶段，而且从罪刑相适应的角度看也是合理的。例如，非法获取公民个人信息罪的法

① 参见张明楷：《刑法分则的解释原理》，北京：中国人民大学出版社，2011年，第347页。

② 小数据（iData），是指围绕个人为中心全方位的数据，及其配套的收集、处理、分析和对外交互的综合系统。（参见《小数据大时代，数据革命迫在眉睫》，2013年12月17日，http://www.36dsj.com/archives/5215，2014年6月12日）

定刑是“三年以下有期徒刑或拘役，并处或单处罚金”；非法获取计算机信息系统罪有两个量刑幅度，情节严重情况下第一量刑幅度也是“三年以下有期徒刑或拘役，并处或单处罚金”，但情节特别严重的量刑幅度为“三年以上七年以下有期徒刑，并处罚金”；侵犯商业秘密罪也有两个相同的量刑幅度；为境外窃取、刺探、收买、非法提供国家秘密、情报罪有三个量刑幅度，分别是“五年以上十年以下有期徒刑”、“情节特别严重的，处十年以上有期徒刑”和“情节较轻的，处五年以下有期徒刑、拘役、管制或剥夺政治权利”。从某种程度上讲，非法获取计算机信息系统数据罪中的数据，侧重于解决虚拟财产犯罪的问题，主要保护财产权和经济利益，因此在法定刑设置上与侵犯商业秘密罪的设置相同。但是，大数据体现为各种维度的数据，包括身份、隐私、人身安全、财产安全、商业秘密、商业竞争优势、企业资产、国家情报等，数据的广义使得非法窃取数据的行为表现出不同的危害程度。从更准确进行行为定性和确定刑罚的意义上说，以“非法获取计算机信息系统数据罪”为基本的数据窃取的罪名，同时，以刑法分则中涉及信息犯罪的相关罪名作为支撑，是一个合理的、切实可行的、完整的体系设计。

2. 明确对数据的非物权保护模式

对于信息的保护模式是不同于传统的物权保护模式的。物质和能量都是可以确定归属、并且能够以其自身的存在就体现其价值的，但信息则不同。信息不是单纯的客观的存在，而是主体与客观世界的反映、交换过程。也就是说，割裂地看信息本身，是无法体现出价值的；只有结合了主体对信息的感知和利用，才能体现出信息的价值。因此，对于信息的保护有两个重要方面，一是谁有权获取信息，二是对信息有怎样的使用权利。获取和使用，是体现信息价值的关键环节。

从定义上看，信息是限定了知悉主体范围的特定事项。例如，商业秘密是指不为公众知悉，能为权利人带来经济利益，具有实用性并经权利人采取保密措施的技术信息和经营信息。又如，根据2000年最高院《关于审理为境外窃取、刺探、收买、非法提供国家秘密、情报案件具体应用法律若干问题的解释》第1条，《刑法》第111条的情报，是指关系国家安全和利益、尚未公开或者依照有关规定不应公开的事项。情报是内部事项，也包括内部对相关资料进行知识整理、汇总所得的分析结果。① 上述定义中“不为公众知悉”、“保密”、“未公开”“不应公开”等用语，都从接触、知晓特定范围信息的主体作了界定。信息的意义在于读取信息的主体会接收特定的讯息、消息，而信息的载体并不重要。因此，对信息的保护是从获取途径上进行限制，只有有权主体才能接触并获知某一内容特定的资讯。由此路径，从刑法层面制定针对数据窃取的行为规范，是确立禁止违反信息获取正当权限而非法获

① 参见王存奎、王爱博、谢晓专、罗根连：《情报界定的相关基础理论研究》，《保密科学技术》2013年第9期。

取信息的行为类型，进而对导致具有刑法意义危害后果的行为进行刑罚制裁。

可选择的另一种保护思路，是延续既有的物权保护模式，将与经济利益相关的数据或信息拟制为财产，将其视为一般的物，纳入刑法侵犯财产犯罪的制裁体系。这样的思路会简化行为类型，将非法获取大致等同于盗窃行为进行评价，关注于犯罪对象的非物质性，对盗窃对象进行更细致的研究，以解释其虚拟性和非排他性。但是，这一模式的关键障碍在于信息与财产的转换，以及衡量标准的论证和统一。

将数据视为虚拟财产是没有问题的，但是，在大数据时代会遇到解释上的困难。因为大数据是复杂客体，不宜将其拟制为动产。理由是：其一，数据多样，数据价值是动态和不确定的，无法准确地转换为财产价值。尤其是价值密度低的元数据，来源零散，有待整合，难以确定为财产和测定财产的数量。其二，数据的价值有多重维度，由虚拟财产延伸到人身安全、隐私、名誉、公共秩序、国家安全等非财产层面，财产价值不再是数据的主要价值体现。其三，数据的非排他性导致数据可以为多主体获知，数据价值没有确定归属。例如，个人电话号码属于个人信息，但是可能用多次授权不同商家使用。其四，数据转化为财产的机制不明确，没有办法固定标准。比如，手机位置信息价值几何？

我国台湾地区“电脑处理个人资料保护法”第 33 条规定，意图营利违反第 7 条、第 8 条、第 18 条、第 19 条第 1 项、第 2 项、第 23 条之规定或依第 24 条所发布之限制命令，致生损害于他人者，处二年以下有期徒刑、拘役或科或并科新台币四万元以下罚金。所援引的条文都是对数据获取权限的规定，因此，此条的行为规范是采取了对非法获取行为进行细化的思路。欧盟的 95/46/EC，GDPR 等个人数据保护指令也都是规定获取个人数据的限定条件，并确立数据获取的原则，以实现对于数据的必要保护。可见，对数据的保护或者说对于侵害数据行为的制裁，通过对于非法获取的行为细化，确立行为规范，是可行的数据保护思路。

此外，对数据使用进行限定也是保护数据的重要行为规范。经营者对采集到的个人数据，未经许可进行二次开发利用或者定向强制推销，也是个人信息滥用的方式之一。① 数据使用必须限定在获取数据的正当目的范围之内，并且不能超出授权使用的方式，且终止于正当目的不再保有之时。

3. 数据犯罪罪名体系的构建

区分数据与信息的差异，利用刑法分则现有罪名群建构一个合理的制裁数据犯罪的罪名体系，需要立足于立法和司法两个层面的思维转变。

（1）立法建立双轨并行的“双核心罪名”

从刑事立法的解释看，应修正两个罪名，才能构建起制裁数据犯罪的基本罪名

① 参见胡其峰：《中国移动浙江公司党组书记、董事长郑杰代表：大数据时代更要保护个人信息》，《光明日报》2014 年 3 月 7 日，第 7 版。

或者核心罪名。这一双轨并行的“双核心罪名”，意在制裁一般的非法获取数据行为和利用职务实施的数据犯罪行为。

其一，将“非法获取计算机信息系统数据罪”修正为“非法获取网络数据罪”。具体而言，修正《刑法》第285条第2款“非法获取计算机信息系统数据罪”，去除前提性的技术行为限定。目前，第285条第2款的罪状表述是“违反国家规定，侵入前款规定以外的计算机信息系统或者采用其他技术手段，获取该计算机信息系统中存储、处理或者传输的数据”。这一罪名出现于大数据时代之前，用于制裁大数据时代的数据犯罪存在两层障碍：一是设置了前行行为，即构成犯罪的前提是“违反国家规定，侵入前款规定以外的计算机信息系统或者采用其他技术手段”，而采用其他手段获取数据的，不构成犯罪。二是限定了数据的逻辑边界，即行为只能是“获取该计算机信息系统中存储、处理或者传输的数据”，而获取云端数据等其他数据的不构成犯罪。为建立制裁数据犯罪的核心罪名，建议去除以上两个限定条件，将这一罪名直接修正为“非法获取网络数据罪”，规定为“非法获取网络数据，情节严重的，处三年以下有期徒刑；情节特别严重的，处三年以上七年以下有期徒刑”。

大数据时代刑法应对数据犯罪的主要困境，在于由数据对象引发的网络犯罪体系内部的深化扩展，同时数据犯罪体系与传统刑法分则各个章节中的信息犯罪相关罪名形成交叉。因此，必须使得数据犯罪的罪名体系成为以数据为出发点，形成一个贯穿或者容纳全部信息犯罪的完整体系，不至于出现针对网络数据的某些严重犯罪行为（例如，针对网络数据的间谍行为）无法制裁的困境。尤其是通过对国家或大型企业APT攻击窃取内部核心信息，以达到提升国家战略优势、操作市场、摧毁关键设施等目的的国家情报或商业情报网络间谍行为，① 以及犯罪行为带有国家背景的严重危害国家安全的网络间谍行为，② 需要由数据犯罪的罪名体系予以包容并得到准确评价，以延长刑法打击半径的方式快速建立起大数据时代国家安全、公共安全等的刑事保障体系。因此，必须从数据内容价值着手，进一步关注元数据承载的潜在信息意义。现行刑法中“非法获取计算机信息系统数据罪”中的数据是技术意义上的数据，主要是针对“身份认证信息”等相关相似类型的数据，在大数据背景下，应当以独立的“网络数据”为对象，将数据作为独立于计算机信息系统的对象，就其自身的信息价值进行单独的价值评判，以此为核心罪名的数据犯罪的罪名体系应当而且必须涵盖需要保护的各层次、各方面的法益，突出刑法的保护机能，避免体系性缺漏的出现。因此，非法获取网络数据罪将成为制裁以外部窃取方式实

① 参见张尼、张云勇、胡坤等编著：《大数据安全：技术与应用》，第131—132页。

② 例如“震网”和“火焰”系美国和以色列联手研发的网络武器，发布这两个病毒的首要目的在于搜集情报，感染火焰病毒的电脑将自动分析自己的网络流量规律，自动录音，记录用户密码和键盘敲击规律。（《2012年中国互联网违法犯罪问题年度报告》，2013年1月18日，http://special.cpd.com.cn/n15549540/，2014年6月5日）

施的侵害网络数据信息犯罪的核心罪名。

其二，修正制裁履职过程中的数据犯罪的罪名。《刑法》第 253 条之一的“出售、非法提供公民个人信息罪”和“非法获取公民个人信息罪”，制裁的是履行职务过程中的数据犯罪行为。通过修正《刑法》第 253 条之一的两个罪名，形成打击半径更大的罪名，是制裁发生在履行职务过程中的数据犯罪的根本。具体而言，建议将罪状中的“将本单位在履行职责或者提供服务过程中获得的公民个人信息”中的“公民个人信息”，修正为“数据”。

在数据犯罪体系中，必须重点对基于提供服务而获得各种通信、行为、位置、流量数据等敏感度高、价值密度高的重要信息数据予以类型化保护，同时，刑法的打击着力点应当聚焦于因履行职务而实现对网络数据实际控制的主体，以切实增强刑事打击的效率和效益。“云端如果导致资料外泄，有大部分的原因都要归咎于 IT”，① google、facebook、云服务商、电信运营商等网络服务的提供主体因服务内容和社会地位，必须严防来自于内部的数据信息犯罪。此外，大数据不仅关系到公民个人数据信息安全，更关系到社会和国家的稳定与安全。因此，更需要在对象上扩展包容性，由信息扩展到数据，由个人层面扩展到数据所能包容的所有层面，以严厉制裁履职过程中实施的所有数据犯罪。也就是说，《刑法》第 253 条之一的罪名未来将成为制裁以内部恶意利用方式实施的侵害网络数据信息犯罪的核心罪名。

（2）司法解释抛弃“二元化”和“三点式”解释思维

为激发固有罪名的实践潜力，司法解释对数据的解释应当抛弃两个传统思维和实现两个根本突破：

其一，抛弃以内部数据和外部数据相配合的二元化数据解释思维。即抛弃以身份认证信息和计算机系统内存数据相配合的二元化数据解释思维，这一解释思维实际上是围绕计算机信息系统进行的解释，滞后于大数据时代的技术变革和数据类型的变化。此种解释思路压缩了数据的范围，对计算机信息系统的内在数据而言，将存在于云端的数据等完全予以排除；对身份认证信息而言，实际上是将计算机信息系统的外部数据限定于以验证身份为内容的数据，即身份认证信息，进而将绝大多数外部数据完全予以排除。二元化的解释思路，形式上是在《刑法》第 286 条和第 285 条的数据之间形成了内部数据与外部数据的分工配合，实际上则是以“二元不对接”的方式，排除了绝大多数数据进入刑法保护视野的可能。

其二，抛弃数据必须附着于信息系统功能的“三点式”数据解释思维。具体而言，要突破“限于计算机信息系统内部的、侧重于信息系统自身功能维护的、以访问控制为主要考虑的数据”的“三点式”传统技术思维和认识，不能过于强调数据

① 参见王林：《云端数据遭觊觎 安全问题不容忽视》，2014 年 8 月 5 日，http://cloud.idcquan.com/yaq/60023.shtml，2014 年 9 月 6 日。

必须附着于信息系统功能的技术要求，应当放弃系统思维，完全以网络思维关注和保护数据自身在内容属性上的价值和保护必要性。

鉴于数据的现实意义，现行刑法必须转变传统思维，重视数据犯罪对原有信息保护体系的全面切入，以开放性的姿态为实现现有刑法罪名体系与数据犯罪罪名体系之间的协调提供可能。例如，2010 年修订的《保守国家秘密法》规定了 12 种可能涉及数据信息的违法行为，这些行为由“违法”上升为“犯罪”的标准，根据 2009 年《关于〈中华人民共和国〉保守国家秘密法（修订草案）的说明》，是“严重违规”，而不是“造成严重后果”，意在严厉制裁实践中大量严重威胁国家秘密、国家安全的行为。应当注意的是，《刑法》第 110、111 条的入罪标准不是“情节严重”，但第 253、286 条却都要求“情节严重”或者“造成严重后果”才构成犯罪，由此，在未来以这两个罪名为核心罪名时，势必出现对“情节”和“后果”的把握问题，从而引发刑事制裁中罪名不衔接的问题：同样是数据犯罪，犯罪对象同样是数据，在危害国家安全罪中的罪名中，入罪标准没有要求“情节严重”和“后果严重”，而在扰乱公共秩序罪中的罪名中，入罪标准则台阶更高，要求达到“情节严重”或者“造成严重后果”，从而导致轻罪入罪标准高于重罪入罪标准的现实尴尬。客观地讲，现行刑法中信息犯罪的罪名体系，一方面是对特殊信息予以类型化保护，另一方面也针对不同内容的信息予以充分的价值评价。在大数据时代，伴随着普通的“数据”、“信息”向特殊的“秘密”、“情报”等数据、信息可转换性的快速提升，司法解释应当针对“国家秘密”等信息，以网络数据与特定信息之间的可转换性为出发，从网络数据尤其是集生性数据的知悉限制等方面把握其时代含义，发挥利用传统信息犯罪的罪名对网络数据犯罪进行有效制裁的规范评价机能。

在完成立法和司法两个层面的修正或者转变后，以数据和信息的实质差异为其他相关罪名的解释思路和适用思路，就可以构成一个以“非法获取网络数据罪”和“非法获取数据罪”为双核心罪名，以侵犯商业秘密罪，为境外窃取、刺探、收买、非法提供国家秘密、情报罪，非法获取国家秘密罪，非法持有国家绝密、机密文件、资料、物品罪，故意泄露国家秘密罪，过失泄露国家秘密罪，非法获取军事秘密罪，为境外窃取、刺探、收买、非法提供军事秘密罪，故意泄露军事秘密罪，过失泄露军事秘密罪等 10 余个罪名为支撑的罪名体系，实现大数据时代对数据的完整、有效的刑法保护。

结　　语

中国已成为网络大国，以此为背景，网络安全已上升为国家安全战略，网络安全的基本内容日益显现为国家信息安全，数据安全更是成为国家安全的核心内容之一。2014 年 2 月 27 日，中共中央总书记、国家主席、中央军委主席、中央网络安

全和信息化领导小组组长习近平主持召开中央网络安全和信息化领导小组第一次会议并发表重要讲话。中央网络安全和信息化领导小组的成立，体现了中国在保障网络安全、维护国家利益、推动信息化发展的决心。

网络安全不仅是互联网的物理安全和运行安全，也不仅是信息载体的安全；网络安全的核心应当是信息安全。大数据时代的网络实现了由“计算”到“数据”的重心变换，网络被整合为围绕数据中心的一个数据收集、存储、处理、应用的流程和系统，由此，以“数据安全”为核心内容的“信息安全”成为“网络安全”的基础。从“数据”到“信息”是一个动态转化过程，大数据主要体现为海量数据和非结构数据，拥有独立于网络传输能力和计算能力的巨大价值潜力，也体现为依托网络媒介汇聚的现实数据，既具有国家、社会和个人不同层面的应用意义，更具有政治、军事、经济、生活等方面的利益内容。因此，必须从国家安全的角度、层次和高度，关注数据的动态价值和现实价值，解释国家安全、国防利益、公共安全、社会秩序、个人隐私等信息法益与数据的同质性。

在新的国家安全观的大背景下，建立具有符合中国国家安全现实需求的信息法律体系，已经成为日益急迫的现实问题。构筑中国的网络安全体系，信息法必为重中之重，信息安全法则是核心，而严厉严密制裁侵犯数据、信息犯罪的刑法罪名体系的重构，是维护信息安全、网络安全的基础。网络犯罪的罪名体系必须实现的范式转换，是完善以信息安全、网络数据为出发点和独立关注对象的侵犯数据犯罪的罪名体系。

习近平在中央网络安全和信息化领导小组第一次会议上指出，没有网络安全，就没有国家安全。① 当前，数据犯罪已经成为网络安全的核心威胁，同时，数据犯罪是一个依托于技术数据而辐射至各层次、各方面现实法益侵害的狭长体系，涉及刑法分则各章的实体内容。以此为视角，刑事立法应对数据犯罪的时代策略，是在刑法中增设以数据为犯罪对象的独立罪刑条款，同时，构筑以刑法分则各章中体现为“秘密”、“情报”、“信息”等信息犯罪条款为接应的罪名体系。因此，中国保护网络安全的法律体系的起点和核心，是确立保护数据安全的法律体系，而其关键环节则是建构严厉严密、完整协调的制裁数据犯罪的罪名体系，构筑保障信息时代国家安全的法律屏障。

〔责任编辑：刘　鹏　责任编审：赵　磊〕

① 《习近平主持召开中央网络安全和信息化领导小组第一次会议强调　总体布局统筹各方　创新发展　努力把我国建设成为网络强国》，《人民日报》2014 年 2 月 28 日，第 1 版。

pendent and link up effectively by means of the two core factors in rule of law, "good law" and "good governance." There is a continuing process of interaction between them, and this interaction is the basic representation of the unity between the domestic and the international rule of law. The framework for the interaction of the domestic and the international rule of law comprises three basic points: state actors and the domestic rule of law, international society and the international rule of law, and rule of law interactive media. Their interaction has the characteristics of being two-way, circular, diverse, comprehensive and evolutionary. In the course of their interaction, China should establish its international position and actively participate in the progress of the international rule of law, grasping its discourse rights in the construction of the rule of law.

(6) An Approach to Sanctioning Data Crimes in the Age of Big Data

Yu Zhigang and Li Yuanli • 100 •

In the age of big data, data have become the core factor in networks and data scale has moved toward horizontal convergence and vertical deepening, with cloud computing platforms becoming a technological resource for data mining. Technological change has triggered new concerns for criminal law, though the data scale in current criminal law is backward and out of date in terms of vertical and horizontal trends. To solve this problem, judicial interpretation has attempted to use technology keywords to expand the items subject to interpretation, and judicial practice has also started to explore the expansion of data content. Nevertheless, due to the misdirection of the observation point from which interpretations are made, overvaluing the spatial character of data and overlooking their value as things in themselves creates difficulties in the determination of criminal cases. Construction of a system for sanctioning data crimes in the age of big data should distinguish between data and information on the basis of their essential differences, define the content and boundaries of technological resources as the subject of protection, value multi-endpoint data resources and convergent data applications, touch down from data to specific legal interests, and define a model for protection of the non-real right of data. A rigorous system of tough sanctions for data crimes will enable us to build a legal barrier to guarantee national security in the information age.

(7) On the Social Construction of Language and Meaning *Chen Bo* • 121 •

The dominant idea in 20th century linguistics and linguistic philosophy is that language