【专题:个人信息保护】

个人信息的加密维度:《密码法》实施后的密码应用与规制路径

刘 晗

【摘 要】密码技术的发展和应用关涉国家安全和个人信息权利,也关系到新一轮信息化建设的底层技术架构。随着《密码法》正式实施,我国已经形成了新的加密技术规制框架,将会促进密码在日常网络行为中的使用。这在通过加密技术保护个人信息的同时,也给个人信息保护的法律机制提出了挑战。一方面,在密码普遍使用之后,密码技术及其规制的发展将会影响到个人信息保护中法律对于去标识化和匿名化的判断;另一方面,在用户和平台更多使用加密技术保护个人信息后,公权力机关为履行法定职责而获取加密信息的需求将会与个人涉及信息的基本权利产生更大的张力,因而需要在新的语境下厘清个人自解密义务和网络运营商协助解密义务的具体程度。

【关 键 词】密码法;信息安全;个人信息保护;规制

【作者简介】刘晗,清华大学法学院副教授,法学博士。

【原文出处】《清华法学》(京),2022.3.95~111

【基金项目】本文系国家重点研发计划"面向IPv6的网络空间国际治理联合研发与示范项目"(2020YFE0200500)、国家社会科学基金重大项目"大数据时代个人数据保护与数据权利体系研究"(批准号18ZDA146)和"大数据、人工智能背景下的公安法治建设研究"(批准号19ZDA165)的阶段性成果。

一、导言

密码是保护信息未经授权而无法获得的技术。在信息社会中,密码承担着双重使命:一方面,密码可以用于保护个人或者组织的信息在网络传播中不受截取、攻击、篡改和冒用;另一方面,作为国家安全体系的组成部分,密码致力于保护国家机密和国家安全。在以上双重意义上,密码是网络信息系统的"保护锁"。

正因为密码的重要作用,随着我国互联网技术的快速发展和普遍应用,与密码相关的法治建设也有了重大进展。2019年10月26日,十三届全国人大常委会第十四次会议通过了《中华人民共和国密码法》(以下简称"《密码法》"),2020年1月1日开始正式施行。随着《密码法》的通过,我国已经形成密码领域的法律体系框架。①

与此同时,随着互联网遍及社会生活的各个方面,也随着大数据、云计算等技术的快速发展,个人信息保护也日益成为热点问题,需要法律予以整体性的回应。2021年8月,我国出台了《中华人民共和国个人信息保护法》(以下简称"《个人信息保护法》"),对于个人信息保护的法律规则进行了全面的规定。特别地,《个人信息保护法》规定了加密技术在个人信息保护中的作用。②

在研究两部涉及互联网信息的重要法律时,值得追问的问题是:加密技术在个人信息法律保护的架构中居于何种地位?密码相关的法律和规制体系对于个人信息保护法律规则体系来说究竟意味着什么?在《密码法》明确赋予个人使用加密技术保护个人信息的权利之后,如何调适公权力维护国家安全、公共安全的需求和个人权利之间的平衡结构?对于这些问题,学界目前的研究尚属起步阶段。《密码法》颁布之前,仅在网络安全和信息安全领域有针对密

码相关法律或政策的研究出现;[3]密码法出台之后,规制机构、法学界和法律界在媒体和自媒体上有一些介绍和解读出现,[4]但在法学专业学术刊物中尚付之阙如。

本文基于对密码学基本原理和密码规制既有路径的考察,试图分析《密码法》所带来的中国密码规制的重大变化,并进一步揭示,《密码法》所涉及的并非只有加密技术这个具体领域的规制问题,它还与个人信息保护这个网络法的基础性问题相关,亟需深入的研究和具体的法律建构予以应对。

二、代码即法律:密码的基本概念与规制路径

(一)作为规制对象的"密码"与加密技术

在密码学和《密码法》的意义上,密码并非用户日常使用的账号密码,如手机密码、社交账号密码、银行卡密码、在线支付密码和电子邮箱密码等。[5]《密码法》第2条规定:"本法所称密码,是指采用特定变换的方法对信息等进行加密保护、安全认证的技术、产品和服务。"所谓"特定变换的方法",就是采用某种算法,把肉眼可辨的文字或者信息("明文")变换成无法直接辨认的符号或者符号序列("密文")。例如,信息加密系统中常用的SHA256算法可将任何信息转化成为一个长度相同,但内容独一无二的字符串,并且无法通过逆运算还原;对原文的任何细小改动都会导致数值改变。[6]此种算法即为《密码法》中所说的"密码"之典型例证。

由是观之,《密码法》中所言的"密码"概念包括密码学、密码技术和密码产业。日常生活中人们所说的"密码"如同钥匙,用来打开具体的锁具。而《密码法》中的"密码"(Cryptograph)[7]则是指加密解密方面的技术、服务和产品,包括密码学和密码学的实际应用,因而更类似于制作各种锁的技术和学问、上锁和开锁服务,以及各种锁具和钥匙。因而《密码法》所管理的对象,是加密解密的底层技术架构、应用形态和相关产业;并且,《密码法》明确相关规制机构的职责,及其相应的法律关系。[8]

《密码法》对于密码功能的界定反映了密码学技术的基本功能:加密和认证。正如《密码法》第2条所言,"密码"一方面能给传递信息提供"加密保护",即将明文信息变成密文信息,防止信息泄露、被人窃取或者篡改;另一方面,密码也可以提供"安全认证",即保证信息发送主体真实可靠,防止欺诈和误解。

正是因为密码的加密和认证功能,密码作为人类信息传输安全的重要技术保证,几乎关涉一切社会领域——无论是政治场景、商业交易还是个人生活,密码都可以满足人们实际的安全需求和心理上的安全感。[9]在信息时代,人们可以使用经过加密或者带有加密功能的电子设备(如智能手机)或者软件(如操作系统、电子邮件程序)进行安全有效的通信,从而保护自己的私密领域不受外界侵犯,从而维护其人格尊严和披露信息的选择自由。可见,密码是个人隐私的有力保护手段,其在某种意义上甚至比法律制度更为有效。很多时候,窃密者即便能够突破法律或者违反法律,也因无法违反数学规律而导致其不可能窃密成功。值得注意的是,密码的使用也有其"暗面":它也可以被犯罪分子、黑社会、颠覆力量乃至于恐怖主义者利用,用以躲避政府追查和法律制裁。

现代密码学基于数学算法设计出了各种加密技术。加密过程依赖的算法,核心即是通过某种函数将信息转化为数值,从而实现从明文到密文的转换。[10]为了达到保密效果,现代密码学通常运用单向函数(one-way functions)或者陷门函数(trapdoor functions)[11]来保证运算的过程在工程上不可逆:明文经过函数运算得出的密文,无法通过同一函数反向计算从而得到明文。需要说明的是,此类函数算法也并非完全无懈可击,而只是要保证试图窃取信息的一方难以在短时间内暴力破解,也即"算法上不可行"(computationally infeasible)。一种算法是否能够达到此种程度,取决于现有的人类算力。[12]当下被认为是安全的加密算法,很可能随着人类算力的增强(例如量子计算的发展)而变得可以轻易攻破。

实践中,信息网络系统特别依赖于不同于传统对称密码技术的非对称加密技术体系。比如,RSA加密算法可用于数字签名和数字证书等身份鉴别技术,保证身份的真实性和不可否认性,防止身份假冒和抵赖;同时还可通过数据摘要技术保证信息完整性,防止篡改。[13]如果说网络安全是整个互联网的免疫系统,密码便是其中的关键基因。

之所以如此,是因为相比较传统的通讯方式(如邮政或者电话系统),互联网通信本身在安全和隐私

保护上较为脆弱，其采取的是分布式网络和包交换通信方式。[14]如若试图保证互联网安全，就必须采用加密技术。对社会生活而言，加密技术在互联网时代就变得前所未有的重要和关键。

(二)加密技术规制的基本形态：国际与比较的视角

正是因为非对称密码的出现，针对密码的法律规制开始成为问题。[15]在非对称密码出现之前，密码技术基本属于国家垄断技术，主要用于军事通信和国家安全事务，并无法律规制方面的问题，而是军政机构的内部管理问题，且普遍采取严格管控的态度。随着非对称密码的出现以及大规模的商用化和民用化，密码技术从军政机构手中相对独立出来自行发展，密码的规制、政府的边界、个人的自由和产业的发展，才成为法律和政策上至关紧要的问题。

从凯撒到美国国家安全局，密码在绝大多数情况下，都曾是主权者或现代主权国家的专用技术。非对称密码发明后，随着大规模的商业化应用，密码广泛成为军民两用产品(dual-use good)，特别是伴随着互联网商业化和社会化运用，密码技术开始成为重要的商用与个人使用的技术。

需要注意的是，在现代密码学中，技术并非完全中立，特别是非对称密码算法天然带有“强化隐私、弱化规制”的政治立场。由于非对称密码系统对个人信息和隐私的保密功能越来越强，私人通信之间开始形成一种相对不受公权力介入和干涉的自主空间，政府因此开始逐渐失去对密码技术的全面垄断。密码领域从政府控制领域，转变为处于政府和市场之间的规制区域。而且，发明非对称密码的密码学家基本都是信奉自由意志主义者(libertarian)和无政府主义的“密码朋克”(Cypherpunk)，[16]倾向于抵制规制、塑造自由空间，使得政府规制本身更加成为问题。更加值得注意的是，非对称密码同样可用于非法活动的保密，公权力机关自然也有更强的动力规制密码。[17]

于是，在政府对商用密码的规制和进出口限制问题上，产生了公权力和私领域之间的激烈冲突。在互联网商业化开始的20世纪90年代，美国曾经出现政府和密码学界的一场激烈冲突，常被称为“密码圣战”(Crypto Wars)。[18]一方坚持打击犯罪，希望在法律和技术上严格管控密码软件的国内使用和国际贸易；另一方则坚持言论自由和隐私权，极力反对政府的规制。这场战争最终以美国政府退缩而告一段落，由此也型构了当代美国密码的规制体系。[19]

美国密码战揭示出来的重要信息是：在数字经济和信息时代，密码作为军民两用技术，同时涉及国家安全和个人隐私。正因为如此，国际社会和各国法律对密码都已经采取了规制措施，其基本原则可以概括为：对于涉及国家安全的密码采取严格管制态度，而对于涉及商业和个人使用的密码则放松管控。

首先，国际社会已经有相关协议对密码的进出口措施予以管理。1996年，33国共同签署的《瓦森纳协定》提出，“通过促进常规武器和双重用途货物和技术转让的透明度和更大的责任，为区域和国际安全与稳定作出贡献……”具体而言，《瓦森纳协定》规定，对56位密钥长度以上的对称加密产品，以及512位密钥长度的非对称加密产品，签订协议各国不得设置出口限制。此外，瓦森纳协议还规定了个人使用豁免，即允许个人出国旅行时携带密码设备供个人使用。经济合作与发展组织(OECD)于1997年也制定了《经合组织密码政策指南》(OECD Guidelines for Cryptography Policy)，[20]其基本目的是在维护国家安全和社会公共利益的前提下，促进密码的商业化和社会化使用。

在国家层面，美国密码法律和政策体系的总体目标可以概括为：(一)增强产业国际竞争力，通过法律和政策，促进美国高科技产业的国际市场占有份额和实际影响力的提高；(二)维护国家安全，限制和打击罪犯和恐怖分子利用强加密技术来开展违法活动。[21]秉承两个目标，形成于20世纪末“密码圣战”之后的现行美国密码法和密码规制体系，总体原则可以概括为：内部使用自由和对外出口管制。[22]我国有学者曾经将其概括为“内外有别”原则。[23]具体而言，美国法律对于密码产品和技术在国内的研发、使用和销售并不加以限制。密码技术的研发和应用被当成“言论”而受到《美国宪法》第一修正案的保护；[24]个人的加密信息在刑事程序中受到第四修正案和第五修正案保护，[25]即执法机关不得非法搜查，以及强迫自证其罪。美国联邦法院曾经判定，刑事案件的侦

查过程中，个人密钥或密码并无针对执法机关的披露义务。[26]

另一方面，在美国，密码产品和技术的出口历来受到法律规制。[27]美国商务部工业和安全局(BIS)负责执行《出口管理条例》(Export Administration Regulations)，其中的管理范围即包含密码产品和技术。该条例设置的商品管控清单中，第五类第二部分“电信和‘信息安全’”一栏规定，除用于医疗终端或者知识产权保护目的的密码产品外，密码产品必须接受出口管制。[28]具体的管制标准主要考量两个因素：一是密码软件的加密属性，特别是密钥长度；[29]二是软件出口的目标客户，也即消费者的属性和国别。[30]

欧盟与美国类似，遵循《瓦森纳协定》设立规则，也在密码治理中采取“内外有别”的原则。[31]一方面，对于国内个人和企业使用密码，欧盟法律奉行自由使用原则，甚至比美国的标准还要更宽松。如同欧盟对个人信息和人格权的保护高于美国标准，欧盟也将密码和密码学提高到事关隐私和人格尊严的层面，进行严格保护。[32]

另一方面，出口管制法规根据欧盟作为跨国联盟的性质，针对不同国家采取“差序格局”的做法。首先，欧盟加盟国内部自由流通和使用，欧盟以外国家进行出口管制。其次，对于欧盟以外的国家，相对管控较轻的是美国、加拿大、日本、新西兰及未加入欧盟的欧洲国家(如挪威和瑞士)等国。对于出口到这些国家的密码产品，需要申请“欧盟一般出口授权”(CGEA)。最后，对其他国家则采取较为严格的管制，需要一事一议地申请对特定国家的出口许可。

三、旧瓶新酒：密码法律体系的基础框架

(一)从商用密码的兴起到《密码法》：中国密码法律治理体系的发展

在我国，密码也是一种两用技术。密码与国家安全、民族独立和军事实力密切相关：如果说互联网是涉及国家主权和安全的第五疆域，密码便是一种重要武器。密码行业也属于高科技研发和应用行业，相关产业的国际影响力对于国家乃至于社会来说也非常重要。数字经济的运行发展，数字生活的正常开展，都离不开密码技术和密码行业：无论是金融、通信、交通、健康、能源，还是公安、税务、社保、电子政务等领域，更不用说物联网、云计算和区块链等新应用场景。[33]

与世界其他主要国家类似，我国密码规制的发展，亦经历了从全面管控到军民两用分别治理的发展历程。长期以来，密码一直是军事国防和外交情报领域的专用技术，几乎没有民用和商用的空间。20世纪90年代，随着市场经济和信息化的发展，社会对保护非国家秘密信息的需求逐渐增大，民用和商用密码的市场空间也随之拓展开来。然而，当时我国的密码技术几乎全部应用于军事和国家安全系统，甚少民用化和商用化，商业密码技术和产业处于起步阶段。例如，当时各大银行使用的多是进口密码机。[34]

顺应社会发展趋势，中央决策机关开始推出相关政策，旨在促进商用密码发展和管理。1996年7月，中共中央政治局常委会研究决定，大力发展商用密码，加强对商用密码的管理。中央办公厅印发《关于发展商用密码和加强对商用密码管理工作的通知》，确定“统一领导、集中管理、定点研制、专控经营、满足使用”的发展和管理方针；同时，从体制层面，确立商用密码管理机构——国家密码管理委员会及其办公室。1999年10月7日，国务院颁布并施行《商用密码管理条例》，开始密码管理的法治化进程。2002年，中央机构编制委员会批准国家密码管理委员会办公室下设商用密码管理办公室，专司商用密码管理。2003年9月，中央办公厅、国务院办公厅联合印发《关于加强信息安全保障工作的意见》(中发办[2003]27号)，首次明确密码在信息安全中的关键作用。[35]由此，在21世纪初，中国初步形成了以《商用密码管理条例》为核心的商用密码治理体系。

随着数字经济和网络安全的发展，以《商用密码管理条例》为核心的旧体系日益变得无法适应新的需求。《商用密码管理条例》比较偏重管制，将商用密码也作为国家机密进行专控管理，密码产品的生产、销售和进出口都实行严格的行政审批制度。[36]例如，国内企业进口密码产品，或在中国境内营业的外资企业要使用外国密码产品，都须向密码管理部门申请备案。近年来，国家推行“放、管、服”政策，转变政府职能，努力优化营商环境。[37]密码领域也得进行相应管理改革，特别是在商用密码领域，政府要做到减轻规制、促进服务。

于是,《密码法》应运而生,成了中国密码法治的重要历史节点。值得注意的是,《密码法》的制定同时建立在中国自主密码技术大力发展的基础之上。[38]从技术角度而言,在20世纪90年代美国进行"密码圣战"的时代,中国现代密码学的发展仍然处于起步阶段,基本停留在对称密码技术。21世纪以来,随着"国密算法"的推出,我国的密码技术已经取得了重大进展。

(二)《密码法》基于密码两用性质的分类管理

任何法律的具体规则都服务于总体的立法目标。《密码法》的总体思想是区分密码的双重性质,分别加以管理:加密技术事关国家安全,必须接受党和国家统一领导;加密技术同时关乎公司和个人的信息安全的,需要加以适度规制,以保护社会公共利益和个人合法权益。具体而言,涉及国家安全和社会公益的加密和解密技术,实行进口许可、出口管制。

遵循密码同时具有军用和民用的双重特点,《密码法》首先对于密码采取分类管理,把各种密码技术和产品分成三大类:核心密码、普通密码和商用密码。[39]核心密码和普通密码保护国家秘密信息:核心密码涉及国家机密,关乎国家安全[40]和国防利益,对应的最高密级是绝密级;普通密码是政府部门使用,对应最高密级为机密级。由于核心密码和普通密码与国家安全紧密联系,《密码法》采取严格统一管理的总体原则,[41]具体制度由国家密码管理局[42]和中央军事委员会[43]制定。《密码法》有关核心密码和普通密码的规则体系建构,改变了此前依靠政策进行管理的局面,大大推进了该领域的法治化进程。

值得说明的是,密码本身和国家秘密并非一回事情。密码本身乃是一整套用于加密解密信息的计算机代码,而国家秘密则是需要加密解密的信息内容本身,且是涉及国家安全和核心利益的一类机密信息。商业密码则是用于企业、组织和个人,涉及非国家秘密的信息。《密码法》规定,在不涉及国家安全和公共利益的密码应用中,放松规制,鼓励和促进技术研发、学术交流和产业发展,并着力推进标准化和国际化。之前《商用密码管理条例》则规定:"商用密码技术属于国家秘密。国家对商用密码产品的科研、生产、销售和使用实行专控管理。"[44]从《商用密码管理条例》对商业密码的属性划分,到《密码法》的分类管理,反映的是法律体系对于密码(学)的认知突变。总体来看,《密码法》对于商业密码规制的核心在于放开主体区分,转而采用行为区分:不再通过设置主体的进入门槛来规制,而是鼓励进入该领域之后,对进入之后的行为进行规制,体现出从事前审批到事中事后规制的转变,甚至在密码技术的开发使用方面呈现某种"促进法"的特征。

从技术角度来讲,分类管理避免了之前不加区分的统一监控政策可能会造成的不便。具体而言,我国自主开发的国密算法安全程度很高,但使用成本也很高,如国密算法不兼容主流浏览器和操作系统。根据《密码法》的新规定,商用密码可以根据使用场景划分安全等级,对使用国密算法还是国际算法具有选择空间。换言之,在商用密码的选择问题上,法律摈弃强制原则,采取"助推"(nudge)[45]模式,鼓励商业组织自愿选择国家标准算法。[46]

进出口管理中的"大众消费类密码产品"例外条款同样体现了《密码法》区分双重用途、适度规制商用密码的倾向。进出口管理是各国密码规制的重要制度之一。《密码法》不再对商业密码进出口管制进行主体区分,而只进行类型区分:对涉及国家安全、社会公共利益且具有加密保护功能的,实行进口许可,出口管制;不涉及国家安全和公共利益的"大众消费类密码产品"则不实行进口许可和出口管制。普通人使用或接触到的密码产品(如手机操作系统里的加密技术和功能和U盘和移动硬盘中的加密技术)不受进出口许可和管制的限制。带有加密功能的大众消费品不再需要冗长繁杂的审批手续,产品在中国上市速度可以加快。

四、法律前沿:加密技术、规制与个人信息保护

《密码法》确立的新规制体系不但对商业主体来说非常重要,对个人用户来说也很重要。因此,《密码法》的实施必将推动密码治理格局乃至于公权力/私权利关系的结构性转变。随着《密码法》的实施和网络用户加密意识的提高,加密技术的广泛运用趋势已经不可逆转,政府权力与个人信息权利之间的冲突将达到前所未有的程度,亟需相关法律予以应对。

(一)密码使用、加密技术规制与个人信息保护

1.《密码法》与密码使用权

密码不但涉及国家安全和经济发展,也涉及通

信自由、通信秘密和信息隐私等公民权利。随着《密码法》的出台和个人信息加密意识提高，公民通过使用加密技术和软件防止通信泄密的倾向势必会变得越来越强。而且，随着网络空间与物理空间不断融合，对密码的使用需求已经扩及每一个互联网用户。用户可以使用密码技术、产品和服务进行网络购物、登录在线银行；密码可以保护静态数据(如手机和个人电脑硬盘中存储的数据)、动态数据(网银交易、网页浏览和电子商务等通过互联网或局域网传输的数据)和平台数据(为保护用户隐私，平台与用户之间的通信使用端到端的公钥/私钥系统加密，因而平台不能访问用户信息，除非用户明确同意)。

毫无疑问，法律赋予公民和法人密码使用权，将极大改变目前大数据时代信息储存和传输过程中大面积不受加密保护的状况。[47]目前，很多数据都是以明文传输和储存在网络系统和大数据系统中。特别是在云计算环境下，用户数据保存在云端，而保存在云端的数据副本常常未经过加密存储。攻击者可以在无需攻破用户个人口令的情况下，从大数据系统中获取数据副本，甚至开展违法犯罪活动。数据泄露多发的现象，很大程度上即源于此。如若加强原始数据在传输和存储中的隐私保护，甚至保证大型公共系统不受攻击，加密技术的运用必不可少。

在此大背景下，个人对于密码的使用权呼之欲出。《密码法》第8条第2款规定："公民、法人和其他组织可以依法使用商用密码保护网络与信息安全。"该条规定为个人使用密码的权利提供了法律权源。根据国家密码管理局的相关解读："公民、法人和其他组织可以依法使用商用密码，既是《密码法》赋予公民、法人和其他组织自主选择使用商用密码的权利，也是鼓励公民、法人和其他组织依法使用商用密码保护网络与信息安全。"[48]

2.加密技术与个人信息保护

不言而喻，密码使用权也与个人信息权密切相关。正如我国著名密码学家王小云教授所言："密码技术是……信息保护的重要手段。"[49]由于密码和加密技术会起到促进数字经济和个人生活等方面的作用，密码使用权利和个人信息权利的保护问题将变得更加重要。2018年7月，中央办公厅、国务院办公厅发布的《金融和重要领域密码应用与创新发展工作规划(2018-2022)》(厅字[2018]36号)特别指出："在互联网应用、云服务和智能终端中，加强密码对公民个人信息和数字资产的保护。"2021年出台的《个人信息保护法》将加密技术与个人信息的法律保护机制相衔接，在具体的法律保护机制(如知情同意等规则)之外，着重规定个人信息处理者使用加密技术的制度，为个人信息的保护提供了一条技术支撑的路径。[50]

作为中国个人信息保护领域的基础性法律，《个人信息保护法》中对于个人信息处理者的加密义务居于重要地位。具体而言，该法要求个人信息处理者必须采取密码技术和去标识化等安全技术措施来保护个人信息在数据静态存储和动态传输中的安全和权利。对于个人信息处理者而言，运用加密技术也是安全性较高而成本较低的一种合规举措。此外，相关技术标准也做了类似的要求。《信息安全技术个人信息安全规范》(GB/T35273-2020)6.3条规定，传输和存储个人敏感信息时，应采用加密等安全措施。

加密技术不仅体现在《个人信息保护法》第51条中规定的"加密"义务中，也体现在该条规定的"去标识化"义务中。原因在于，作为一种信息技术，去标识化大量使用了各种加密技术。例如，《信息安全技术个人信息安全规范》(2020)3.15条规定，去标识化的方式有假名、加密和哈希函数等技术手段；《信息安全技术—个人信息去标识化指南》(GB/T37964-2019)中列举的常用去标识化技术也包含密码技术。

3.加密技术及其规制对个人信息保护的挑战

然而，在加密技术助力个人信息保护的同时，它也给个人信息保护及其法律规则带来了新的挑战，甚至对于互联网信息和代码规制提出了新的问题。

究其实质，个人信息保护需要放在数字经济的大格局下进行定位，因此存在与促进数据流通、跨境流动和开发利用等问题的潜在张力。《个人信息保护法》虽然并未处理此问题，但这种张力及其平衡在《数据安全法》以及一系列数据政策当中明确地体现出来。《个人信息保护法》及其相关规则体系确立了以授权同意和去标识化为核心的规则体系，在保护用户权利的同时，自然对于数据流通和开发利用产生了一定的抑制效应。反之，一旦数据流通之后，其他主体若可以通过解密技术反推，从而还原原始数

据，突破个人信息去标识化和匿名化的限制，就会使得个人信息权利重新受到巨大威胁。

目前，互联网产业界通过数据标识加密技术、关联技术和有效授权技术，尝试确保个人敏感信息不可识别和仅在授权范围内使用，为个人信息保护提供了技术保障。加密技术的使用不仅有助于个人信息保护，也有助于企业和技术社群在进行数据流通和开发利用过程中设计合规方案。尤其是2020年以来，部分是为了平衡个人信息保护和数据流通利用之间的关系，以密码技术为重要支撑的“隐私计算”技术方兴未艾，并在数字经济中得到应用。融合了密码学和其他计算机科学的隐私计算可用于加强数据流通过程中对个人标识信息的加密保护，从而促进数据流通价值和个人信息保护之间的动态平衡。[51]具体而言，该技术通过对于个人信息的加密，可以实现在原始数据留存本地的基础上，通过技术化手段只输出切片、标签化、脱密后的梯度和参数等信息满足去标识化的要求，使得其他数据处理者不能够复原数据中包含的个人可识别信息，从而实现数据流动和他者的联合开发。而且，一旦满足了去标识化的要求，个人信息处理者及其他数据使用者也可以免除使用数据进行分析过程中征求用户二次甚至多次授权的麻烦，从而能够一定程度上符合《个人信息保护法》的合规要求。[52]

然而，以隐私计算为代表的新兴数据处理技术却面临着法律评价上的不确定性。毕竟，此种技术仍然属于《个人信息保护法》中的去标识化技术，而非匿名化技术。它可以降低个人信息的敏感程度，但并非使得个人信息在传输和流通之后完全不可识别，因此仍然需要在个案中判断该技术能否能够帮助个人信息处理者达成合规义务。[53]而对此问题的判断，不但取决于《个人信息保护法》的相关实施细则和相关技术标准，也取决于《密码法》背景下的加密技术发展(例如当前认为足以去标识化、无法识别个人身份和属性信息的技术，是否可能随着技术的迭代，变得可以识别，再如加密过程中的密钥被获取或密码系统被破解的难度是否随着技术的发展而降低)，甚至取决于《密码法》所建构的规制体系下的具体规制措施和个案处理。因此，网络运营商作为个人信息处理者和加密技术使用者，也要不断根据算法和个人信息保护的场景，对于其所使用的加密技术进行安全认证，从而符合《密码法》等法律建构的加密技术规制规则体系。

更有甚者，技术的发展及其应用也会不断挑战《个人信息保护法》体系中预设的去标识化和匿名化的二分法。[54]按照该法规定，去标识化的信息在经过额外信息辅助的情况下(如获取对于个人信息数据进行加密的密钥)，仍然可以复原为个人信息。去标识化仅是增加了识别自然人身份和属性信息的难度，而非排除了其可能性。匿名化则意味着个人信息数据无法复原。加密解密技术的发展完全可能产生一种现象，即原先无法复原的数据可以通过新的技术予以复原，从而影响《个人信息保护法》的适用范围——该法第4条规定，匿名化信息不属于该法保护的个人信息。此时，是否应该在《密码法》之下的加密规制体系中限制此类代码的开发和技术的使用，就变成极为关键的问题。就此，法律需要在个案当中判断一项加密技术是否满足了匿名化的要求，从而免除《个人信息保护法》设定的义务，还是仅仅起到了去标识化的作用，以及作用有多大，从而确定个人信息处理者已经履行了该义务。个人信息保护法领域的学者和实务人士因而必须直面密码技术的更新迭代，并且关注密码规制的发展状况。

(二)执法需求与个人信息的平衡机制：法律与技术的交叉路径

1.密码的社会化使用与执法需求的张力

必须注意的是，加密技术的普遍社会化使用是一把双刃剑。加密技术的个人使用普遍化将会打破公权力和隐私之间的既有平衡状态。随着《密码法》的推行，公众对密码技术的认识和运用加密技术保护个人信息和隐私的程度提高，会造成执法和司法机关获取数据的技术困难。究其实质，互联网从其底层架构而言，“易攻难守”。[55]加密技术在信息网络各个环节的普遍使用，会使互联网的攻守态势趋于平衡。然而，新的平衡将会带来执法与隐私之间新的不平衡。加密技术的广泛使用，不但意味着个人信息隐私得到更强保护，也意味着公权力机关获取数据的难度相应增大。这个难题已经超出了传统的政府维护安全的权力和个人的隐私权利之间的冲突框架，[56]也构成了公共安全和个人信息安全之间的冲

突。[57]此外，更需注意的是，个人信息安全也不仅牵涉个人隐私，同时也关涉社会利用网络信息系统进行发展的整体利益(例如数字经济和数字治理)。

公权力与隐私之间的冲突典型地体现在执法机关为打击犯罪而获取数据的过程之中。在大量数据未加密的情况下，张力尚不明显。然而，一旦加密普及开来，执法机关将会面临重大障碍。毕竟，越来越多的数据将会以密文形式传输和存储，有效防止截获、泄露和篡改。[58]第三方(无论是攻击者还是执法者)获取数据的难度会不断加大。从国外经验来看，执法机关可能采取的措施分为两大类，一是寻找密钥进入系统获取数据，二是在不获取密钥的情况下直接获取数据。[59]前者则进一步区分为找到“密码”(口令)、暴力破解和通过侦查、审讯嫌疑人获取“密码”；后者则包括利用加密系统漏洞予以破解、在设备使用时获取明文数据和获取数据在运营商上的备份。[60]无论何种方法从数学原理来说都只是概率性的，无法提供一通百通的方法，也没法决定优劣之分，因为对于方法的选择取决于执法机关的技术认知程度、技术使用能力高低和资源配置程度。[61]在极端情况下，执法机关面临着数学法则的制约。[62]例如，在网络服务提供商并未保留用户私钥的情况下，在端对端加密通信中，执法机关需要借助极强的算力资源方才能够实现其目标。[63]甚至在某些情况下，执法机关的解密效果与加密技术的规制密切相关，特别是法律对于个人使用商用密码的强度(特别是密钥长度)的规定。[64]

以2016年Apple v. FBI案为例。苹果公司被FBI依法要求协助破解圣贝纳迪诺袭击者赛义德·法鲁克(Syed Farook)使用的iPhone 5c手机。法鲁克已死，使得执法机关强迫其提供密钥的策略无法进行。政府知道，法鲁克的手机启用了自动删除功能以阻止暴力破解，盲猜“密码”就变得更难。政府转而试图获取明文数据的备份副本，并获得了手机内容在云端(iCloud)上的备份，但云端存储的只是6个星期之间的较早版本，而FBI希望获得最新的副本。FBI获得法院许可，要求苹果公司协助，禁用云端副本的自动删除功能，以便快速猜测破解密码，实际上就是让苹果公司“开后门”。苹果公司反对，认为这会侵犯用户隐私，丧失其他用户信任。[65]FBI最终另辟蹊径，在诉讼判决之前，通过匿名的第三方协助破解了密码。

上述案件体现出来的是在执法机关获取数据的场景中典型的问题所在，即一方面，犯罪嫌疑人是否有法律上的自解密义务；另一方面，互联网运营者、设备制造商乃至于加密算法开发者的协助解密义务问题。

2. 可能的解决方案：自解密义务与协助解密义务的范围与限度

为了应对执法困局，技术与法律相结合的方案在世界范围内已经有所发展，其中有两种方案值得加以探讨。一是在个人使用的加密算法中要求算法开发者设立“后门”。例如，澳大利亚曾经出台反加密法，允许政府强迫科技公司为产品设置后门。[66]具体而言，此种开发“后门”的法律义务设定，如果加密系统中不设置执法部门可以获得明文的技术机制，该加密系统不得推广使用。但是，此举风险很大，仍需慎重。首先，从技术角度而言，开“后门”是双刃剑，具有较大的潜在风险。本国执法可以从“后门”进入系统，外国政府、黑客甚至恐怖主义者也可以从“后门”进入。这反倒会导致网络信息安全赤字。其次，从经济角度而言，开“后门”将会威胁个人信息和隐私保护，减少本土加密产品和网络安全产品的国际市场需求，也不利于一国密码标准的国际化，甚至可能因为违反外国隐私法而面临诉讼、合规乃至公共关系的风险，有损产业的国际竞争力。[67]尤其是考虑到未来物联网和区块链的发展都要依靠密码标准，此举更得慎重。[68]最后，不言而喻，“后门”制度本身也会产生舆论争议。[69]

另一种做法是设立国家密钥托管系统。[70]其初衷是，公权力机关出于维护国家安全和公共安全的义务，须有某种数据恢复的权力，其中包含获取加密数据的权力，特别是通过预设数据恢复密钥，获取相应数据，来打击犯罪和危害国家安全的行为。此种备用密钥系统也对个人用户的密码使用权利有所帮助，它可以协助用户在丢失私钥之后解决问题。例如，20世纪90年代，为了缓解安全和隐私之间的冲突，克林顿政府曾经试图建立美国的国家密钥托管系统，希望在保证个人信息隐私的同时，为打击犯罪和恐怖主义等行为提供技术手段。此举并非将网络用户的“口令”进行统一管理，而只是从算法层面管

理密钥生成的算法机制，以便必要时公权力机关可获取具体“口令”。然而，密钥托管系统遭到了法律界和产业界的集体反对，最终无法推行。

在《密码法》和《个人信息保护法》出台之前，我国法律中并未规定对于犯罪嫌疑人的自解密义务。在司法实践中，不配合解密行为常常比照刑法中的妨害公务罪或《治安管理处罚法》中拒绝、阻碍国家工作人员依法执行职务的行为。[71]在两部法律出台之后，特别是其中对于使用加密技术保护个人隐私和个人信息的权利进行强调之后，以往的做法显得不甚妥当，因此需要在法律层面就自解密义务和协助解密义务进行更为明确的制度设计。

就目前的法律而言，针对涉及国家安全案件中的解密义务问题，已经有了较为明确的规定。如《反恐怖主义法》(2018年修正)第18条明确规定：“电信业务经营者、互联网服务提供者应当为公安机关、国家安全机关依法进行防范、调查恐怖活动提供技术接口和解密等技术支持和协助。”因此，在涉及恐怖主义的案件中，电信业务经营者和互联网服务提供者具有协助解密义务。而2015年《国家安全法》第77条第1款第5项规定公民和组织有义务“向国家安全机关、公安机关和有关军事机关提供必要的支持和协助”。在涉及使用加密技术的案件场景中，该条款可以解释为在国家安全案件中，公民和组织有自解密和协助解密的义务。相较而言，2016年通过的《网络安全法》第28条规定：“网络运营者应当为公安机关、国家安全机关依法维护国家安全和侦查犯罪的活动提供技术支持和协助。”该条款似也可以作类似解释。

如果说在涉及国家安全的案件中，解密义务存在与否的问题较为明确，那么在普通刑事案件的侦查中，相关法律的规定并不明确。上文提及的《网络安全法》第28条的规定虽然为网络运营者设置了“提供技术支持和协助”的义务，但该义务是否包含解密义务，其义务的强弱程度如何，法律并未明言。可以肯定的是，该条款并未为公民个人设置自解密义务；而且，由于自解密义务涉及公民在宪法上的通信自由和通信秘密权，同时也与不得强迫自证其罪的刑事诉讼法原则存在潜在的冲突，因而可以相对确定的是，法律目前并无此种要求。[72]本文建议，未来的制度设计中维持现状、不设定自解密义务是较为妥当的措施。在此基础上，本文认同有论者提出的方案，即司法机关可以要求犯罪嫌疑人采取自愿合作的方式来予以尝试，并在犯罪嫌疑人拒绝配合的情况下，允许法院采信这一事实，[73]从而维护打击犯罪与保护公民基本权利(包括但不限于个人隐私/信息权利和不自证其罪的权利)之间的平衡。

难点在于网络运营者的协助解密义务，这有待于更为细化的制度进行澄清。在此之前，我们仍然可以从法律原理和实践现状的层面进行初步探讨。在原理层面，在处理个人和组织的自解密义务和协助解密义务问题时，毫无疑问应当遵循比例原则，一方面赋予执法机关在特定场景中获取加密数据的相关权力，另一方面从法律上施加程序规范和实体限制，以此平衡政府权力和公民权利之间的界限。[74]实践层面，“在向网络服务提供者要求执法协助的启动点上，司法机关有启动过于频繁、启动阈值过低的问题”。[75]针对于此，本文建议应对于司法机关要求网络运营者解密的行为采取如下限制。

一是最低限度原则。按照《个人信息保护法》第34条的要求，国家机关在履行法定职责时，应当在必需范围和限度内处理个人信息。[76]这一点也应解释适用于司法机关通过解密而获取个人信息和数据的情况。例如，司法机关在原则上只能要求相关主体解密犯罪嫌疑人本人的信息和数据，只有在确为必要的条件下，司法机关才可以要求网络运营者解密与犯罪嫌疑人具有密切关系的人员的相关信息。再如，需要明确网络运营者的协助解密义务在不同案件类型中的相应程度，如只针对涉及重大罪名的刑事案件设置完全的协助义务，而针对一般刑事案件，则需要注意公共利益和个人隐私的平衡。[77]

二是权利保障机制。《个人信息保护法》的宗旨就是确立以知情同意为核心的个人信息权利保护体系，并且特别规定了国家机关在履行职责时处理个人信息过程中对于权利主体的告知义务。[78]此原则也应适用于协助解密的场景中。具体而言，当司法机关在法定范围内依照最低限度原则成功获得网络运营商协助解密当事人的信息之后，当事人有知情权(如公安机关必须告知)和刑事程序性权利(如当事人有权申请排除非法证据)。

三是安全保障义务。按照《密码法》《数据安全法》《网络安全法》和《个人信息保护法》等法律的相关规定，司法机关和网络运营者对在解密过程中获取的国家秘密、商业秘密和个人信息应当尽到保密义务，尤其不得用于与案件侦破无关的用途。

五、结语

《密码法》实施之后，密码治理相关的法律体制将会迎来全面发展，同时也会与个人信息保护相关的法律规则发生密切联动。加密技术的广泛使用究竟会给法律带来什么机遇和挑战，既取决于技术创新(例如量子计算机的出现)，也取决于法律变革(特别是第三方协助义务的法律范围)。对密码治理采取技术与法律结合的研究进路，或许同时具有一定方法论意义。互联网时代，“代码就是法律”。[70]而在“所有东西都是计算机”“万物皆数”的大数据时代，密码是从技术底层保护网络安全和个人信息的重要代码。密码治理的法律问题，已经超越了密码产品的研发、销售、使用和进出口等具体问题，触及了法律制度的根本，即权力和权利的基础关系和根本边界。结合技术与法律两个不同的面向，洞悉信息社会治理的深度结构和底层逻辑，是应对未来密码规制体系和个人信息保护制度的基本思维。

注释：

①在法律层面，除了《密码法》之外，还有《国家安全法》《保守国家秘密法》《网络安全法》《反恐怖主义法》《电子签名法》(2004年通过，2015年第一次修订，2019年第二次修订)和《对外贸易法》等相关法律中的相关条文；行政法规包括《商用密码管理条例》(国务院令第273号)《技术进出口管理条例》(国务院令第732号)和《国务院关于取消一批行政许可事项的决定》(国发[2017]46号)。部门规章层面，包括国家密码管理局制定和公布的《商用密码产品生产管理规定》(2005年通过，2017年12月1日修订)、《商用密码科研管理规定》(2005年通过，2017年12月1日修订)、《电子认证服务密码管理办法》(2005年通过，2017年12月1日修订)、《国家密码管理局关于做好商用密码产品生产单位审批等4项行政许可取消后相关管理政策衔接工作的通知》(国密局字[2017]336号)、《电子政务电子认证服务业务规则规范》(国密局字[2018]572号)等。此外，还有技术方面的国家标准，包括但不限于《GM/T0054-2018信息系统密码应用基本要求》《GM/T0044-2016SM9标识密码算法》《GM/T0045-2016金融数据密码机技术规范》等。

②该法第51条规定：“个人信息处理者应当根据个人信息的处理目的、处理方式、个人信息的种类以及对个人权益的影响、可能存在的安全风险等，采取下列措施确保个人信息处理活动符合法律、行政法规的规定，并防止未经授权的访问以及个人信息泄露、篡改、丢失：……(三)采取相应的加密、去标识化等安全技术措施……”

③参见肖志宏：《我国密码法律体系架构研究》，载《信息安全研究》2018年第9期，第853-856页；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》，载《信息安全研究》2018年第3期，第201-210页；马民虎、王新雷：《试论商用密码管制法之动态国家利益观》，载《信息网络安全》2009年第3期，第47-49页；马民虎、赵婵、冯立杨、王新雷：《商用密码管制：从对立到包容之趋势分析》，载《信息网络安全》2009年第2期，第60-62页、第69页；马民虎、原浩：《密钥托管与公民隐私权的国外立法》，载《信息网络安全》2005年第8期，第62-63页；马民虎、原浩、许苏嘉：《美欧密码进出口监管的“游戏”法则研究》，载《情报杂志》2005年第1期，第9-11页；马民虎：《美国密码出口监管政策的“欧盟”现象》，载《信息网络安全》2002年第3期，第34-36页；马民虎、杜立欣：《内外有别的控制政策——美国密码政策演变轨迹》，载《国际贸易》2001年第10期，第21-23页；马民虎：《美国密码政策的演变轨迹》，载《信息网络安全》2001年第8期，第21-23页。

④参见陈亦超：《构建国家安全法律制度体系的重要环节——〈中华人民共和国密码法〉几个问题解读》，载《中国信息安全》2019年第11期，第56-59页；荆继武：《学习〈密码法〉的体会与思考》，载《中国信息安全》2019年第11期，第69-70页；张宝山：《密码法“亮相”：助力密码工作法治化》，载《中国人大》2019年第13期，第35-36页。篇幅所限，自媒体上的解读文章恕不一一列举。

⑤日常生活中人们上网或者登录电子设备所使用的各种密码，在严格意义上只是“口令”。

⑥该算法广泛运用在数字签名领域，成为电子商务的技术支撑之一。例如，“密码法研究”这个短语，通过SHA256算法计算出来的数值是“e3a0690c4df0310dcf52cf3f62cbd5525186958615df5122849057e2b3e155”。而“《密码法》研究”的数值是“45f274c9af5f95f3d2c31151dbd3f53a531fff64784c6bf3465735b98b80dcd1”。两者之间虽然只是一个书名号的变化，但数值却差别甚大。

⑦严格说起来，Cryptography更应该被称为“密码术”。密码术(Cryptography)是一门用密码(cipher)、代码(code)和相关技术来伪装信息的科学。密码(cipher)是一种不论任何内容都可以加密的方法。代码(code)则是一种编码系统，即一套预先安排好的意义映射系统。而广义上的密码学(Cryptology)是研究密码术(Cryptography)和密码分析(Cryptanalysis，主要是破译密码)的学科。参见[美]Richard Spillman：《经典密码学与现代密码学》，叶阮健、曹英、张长富译，清华大学出版社2005年版，

第3页。

⑧法律并非不保护个人日常生活使用的“密码”，只是不在《密码法》里直接保护。如《最高人民法院关于审理扰乱电信市场管理秩序案件具体应用法律若干问题的解释》(法释[2000]12号)第8条规定：“盗用他人公共信息网络上网账号、密码上网，造成他人电信资费损失数额较大的，依照刑法第二百六十四条的规定，以盗窃罪定罪处罚。”盗号还可能构成侵权行为，如被盗号的主体遭受财产损失，或名誉损失，可主张民事赔偿。

⑨See A. Michael Froomkin, The Metaphor Is the Key: Cryptography, the Clipper Chip, and the Constitution, 143 University of Pennsylvania Law Review 709, 718-719(1995).

⑩See Alfred J. Menezes, Paul C. van Oorschot & Scott A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996, pp. 6-8.

⑪参见同上注,第8-9页。

⑫See Jacob Ziv, In Search of a One- Way Function, in Thomas M. Cover & B. Gopinath eds., Open Problems in Communication and Computation, Springer, 1987, pp. 104-105.

⑬参见左朝胜、马军峰、徐晓颖、高建远：《铸造国家政务安全的云盾牌》，载搜狐网2018年3月7日，http://www.sohu.com/a/225016419_161623。

⑭See David D. Clark, The Design Philosophy of the DARPA Internet Protocols, 18 Computer Communication Review 106, 106-114(1988).

⑮另外一个重要的因素是美国联邦政府将对称密码DES(Data Encryption Standard，一种使用56位密钥的对称算法)于1976年确立为联邦资料处理标准(FIPS)，随即公开传播，甚至在国际社会广泛流传。

⑯密码朋克邮件组(Cyberpunk Mailing-List)于1992年成立，其早期成员包括后来大名鼎鼎的人物：BT下载创始人布拉姆·科恩(Bram Cohen)、维基解密创始人阿桑奇(Julian Assange)、万维网WWW的发明者蒂姆·李(Tim B. Lee)、脸书的创始人之一帕克(Sean Parker)以及比特币创始人中本聪。其基本思想是无政府主义。其中也有少数法学家，如迈阿密大学法学院A.迈克尔·弗鲁姆金(A. Michael Froomkin)教授。其基本思想倾向参见《密码无政府主义宣言》(Crypto Anarchist Manifesto), https://www.activism.net/cypherpunk/crypto-anarchy.html。

⑰《密码法》第12条规定：“任何组织或者个人不得窃取他人加密保护的信息或者非法侵入他人的密码保障系统。任何组织或者个人不得利用密码从事危害国家安全、社会公共利益、他人合法权益等违法犯罪活动。”

⑱See Eric Rice, The Second Amendment and the Struggle Over Cryptography, 9 Hastings Science and Technology Law Journal 29, 31(2017).

⑲See e.g., Bernstein v. U. S. Dept. of State, 945 F. Supp. 1279, 1286(N. D. Cal. 1996).

⑳全称“OECD密码政策推荐指南”(OECD Recommendation Concerning Guidelines for Cryptography Policy)，参见http://www.oecd.org/sti/ieconomy/guidelinesforcryptographypolicy.htm，2020年2月9日访问。

㉑See Tricia E. Black, Taking Account of the World as It Will Be: The Shifting Course of U. S. Encryption Policy, 53 Federal Communications Law Journal 289, 292(2001).

㉒See Nathan Saper, International Cryptography Regulation and the Global Information Economy, 11 Northwestern Journal of Technology and Intellectual Property 673, 679-682(2013).

㉓参见同前注③，马民虎、杜立欣文，第21-23页。

㉔甚至有美国学者认为，由于密码本身是进出口法律中的“武器”，因此也可以享受第二修正案“持有武器的权利”的保护。参见同前注⑱，Eric Rice文。

㉕参见《美国宪法》第四修正案规定，“人民的人身、住宅、文件和财产不受无理搜查和扣押的权利，不得侵犯。除依据可能成立的理由，以宣誓或代誓宣言保证，并详细说明搜查地点和扣押的人或物，不得发出搜查和扣押状”；第五修正案规定，“任何人……不得在任何刑事案件中被迫自证其罪……”

㉖See In re Grand Jury Subpoena to Sebastien Boucher, No. 2: 06-mj-91(D. Vt. Feb. 19, 2009).

㉗美国密码技术和产业世界领先，因此对于外国密码产品和技术并不设置任何进口限制。

㉘See Bureau of Industry and Security, Export Administration Regulations, Commerce Control List, Category 5-Telecommunications and "Information Security", BIS(Dec. 7, 2012), http://www.bis.doc.gov/policiesandregulations/ear/ccl5_pt2.pdf.

㉙参见同上注。

㉚参见美国财政部网站相关信息，https://www.treasury.gov/ofac/downloads/sdnlist.pdf，2020年2月9日访问。

㉛See Setting Up a Community Regime for the Control of Exports of Dual-use Items and Technology, Council Regulation(EC) No 1334/2000,https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32000R1334.

㉜参见同前注㉜，Nathan Saper文，第482页。

㉝比如，在金融领域，规制部门需要通过有效的密码技术手段，打击伪造银行卡、伪造网上交易身份等违法犯罪行为。在税收领域，增值税防伪税控系统也是采用密码技术保护涉税信息，增值税发票上的四个二维码，就是密码技术的应用；二代身份证里面也是使用密码芯片，防止伪造身份证等违法犯罪行为。而网民上网留下的个人敏感信息、隐私，乃至商业秘密，不但需要法律保护，更需要技术保护。参见人民网：《〈中华人民共和国密码法〉发布这六个问题你需要知道》，载

国家互联网信息办公室官方网站2019年10月29日，http://www.cac.gov.cn/2019-10/29/c_1573880702680488.htm。

㉞参见倪俊：《浓缩的中国商用密码产业发展史——卫士通二十年商密业务发展历程》，载《信息安全与通信保密》2018年第5期，第118-130页。

㉟参见《国家密码管理局商密办张平武：商用密码发展历程与展望》，载网络安全等级保护网2018年9月21日，http://www.djbh.net/webdev/web/AcademicianColumnAction.do?p=getYszl&id=8a81825664ceff130165f9c361af0070，2020年2月9日访问。

㊱参见《商用密码管理条例》第13条规定："进口密码产品以及含有密码技术的设备或者出口商用密码产品，必须报经国家密码管理机构批准。任何单位或者个人不得销售境外的密码产品。"此条规定设置了两项行政审批：出口许可审批；进口审批制度。

㊲参见《优化营商环境条例》(中华人民共和国国务院令第722号)。

㊳国外密码产品和服务从供应链角度而言存在风险，国外密码算法占据了世界大部分市场份额(如AES、RSA、SHA256等算法)。

㊴参见《密码法》第6条。

㊵例如，一些新兴的加密通讯软件已经被视为威胁国家安全的工具。参见同前注④，陈亦超文，第56页。

㊶参见《密码法》第3-5条。

㊷《密码法》第42条规定管理密码的核心机构：国家密码管理局。根据2018年3月国务院发布的《国务院关于部委管理的国家局设置的通知》(国发[2018]7号)，国家密码管理局与中央密码工作领导小组办公室一个机构两块牌子，列入中共中央直属机关的下属机构序列。

㊸参见《密码法》第43条。

㊹《商用密码管理条例》第3条。

㊺Richard H. Thaler & Cass R. Sunstein, Nudge: Improving Decisions about Health, Wealth, and Happiness, Yale University Press, 2008.

㊻例如，在非对称密码算法中，鼓励使用国家标准SM2，但也允许使用国际通行的RSA算法，只是要求必须具有相当强度，如2048位密钥，甚至更高。

㊼参见滑明飞：《1400万快递用户隐私裸奔：如何为大数据加密？》，载搜狐网2014年8月18日，http://news.sohu.com/20140818/n403520015.shtml。

㊽国家密码管理局：《密码政策问答(二十二)》，载国家密码管理局官方网站，http://www.oscca.gov.cn/sca/xxgk/2020-01/28/content_1060626.shtml。

㊾王小云：《密码技术是数据治理和信息保护重要手段》，载正义网，http://news.jcrb.com/jxsw/201811/t20181109_1924340.html。

㊿参见《个人信息保护法》第51条。从比较法角度来看，这也是较为通行的做法。2018年出台的欧盟《一般数据保护条例》(GDPR)第32条规定，数据"控制者和处理者"在处理个人数据时，应采取"适当技术与组织措施，以便保证和风险相称的安全水平"，其中第一项即是"个人数据的匿名化和加密"。欧盟《一般数据保护条例》，丁晓东译，https://www.sohu.com/a/232773245_455313。其说明条款(Recitals)第83条进一步规定："为了维护安全和防止违反本规定的处理，控制者或处理者应评估处理中固有的风险，并采取措施来降低这些风险，如加密。这些措施应确保适当程度的安全，包括保密……"General Data Protection Regulation, Recital 83, https://gdpr-info.eu/recitals/no-83/。译文为笔者翻译。欧盟的做法虽然并未规定数据控制者和处理者的违法责任，但也为其处理数据中使用加密技术提供了明确的方向。加拿大《个人信息保护和电子文件法》(PIPEDA，2000)则规定："消费者的个人信息必须由与个人信息的敏感性相适应的安全措施保障，包括使用密码(passwords)和加密(encryption)等技术措施。"如若商业组织违反此条款，则需承担最高10万加元的惩罚。Personal Information Protection and Electronic Documents Act, S. C. 2000, C. 5, https://laws- lois.justice.gc.ca/ENG/ACTS/P- 8.6/page-4.html#h-417174. 相比较而言，美国《加利福尼亚州消费者隐私法》(CCPA)在保护个人隐私的规定中，虽然在运营商的安全保障义务中没有明确提及加密义务，但在相应的诉讼规则中隐含了加密问题。该法第1798.150(1)中规定："任何消费者如其……未加密或未经处理的个人信息，由于企业违反义务而未实施和维护合理安全程序以及采取与信息性质相符的做法来保护个人信息，从而遭受了未经授权的访问和泄露、盗窃或披露"，则消费者可因3项原因提起民事诉讼，其中包括提起每个消费者100美元到750美元之间的赔偿请求。换言之，如果企业采用了对于消费者个人信息的加密处理，则至少可以就此提出抗辩，免除赔偿。See California Consumer Privacy Act of 2018，1798. 150，中文译文参见《美国〈2018年加州消费者隐私法案〉》，吴沈括等译，载"安全内参"2018年7月10日，https://www.secrss.com/articles/3836。

(51)参见隐私计算联盟、中国信息通信研究院云计算与大数据研究所：《隐私计算白皮书》，2021年7月，第2页。

(52)参见同上注，第33页。

(53)参见苏州信息安全法学所：《密码技术在〈个人信息保护法〉中的基石地位和实现》，载安全内参网2021年8月27日，https://www.secrss.com/articles/33841。

(54)《个人信息保护法》第4条规定："个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。"

(55)左亦鲁：《国家安全视域下的网络安全——从攻守平

衡的角度切入》,载《华东政法大学学报》2018年第1期,第155页。

[56]See Cass R. Sunstein, Beyond Cheneyism and Snowdenism, 83 The University of Chicago Law Review 271, 272-273(2015).

[57]See Bruce Schneier, The Value of Encryption, Schneier On Security(Apr. 2016), https://www.schneier.com/essays/archivcs/2016/04/the_value-of_encrypt.html(hereinafter Schneier Ⅱ);Olivia Gonzalez, Cracks in the Armor: Legal Approaches to Encryption, 2019 Journal of Law, Technology & Policy 2,9-10(2019).

[58]参见《专家解读〈密码法〉,数据加密保护将是我国网络安全工作的重点》,载和讯网,https://shandong.hexun.com/2019-10-28/199026576.html,2020年2月9日访问。

[59] See Orin S. Kerr & Bruce Schneier, Encryption Workarounds, 106 Georgetown Law Journal 989, 989-1020(2018).

[60]参见同上注。

[61]参见同上注。

[62]See John Villasenor, No, the Laws of Australia Don't Override the Laws of Mathematics, Brookings Institution(July 17, 2017), https://www.brookings.edu/blog/techtank/2017/07/17/no-the-laws-of-australia-dont-override-the-laws-of-mathematics.

[63]参见同上注。

[64]See Peter Swire & Kenesa Ahmad, Encryption and Globalization, 13 Columbia Science & Technology Law Review 416, 441-444(2012).印度最近的"密码圣战"可以提供参考。随着2008年孟买大爆炸的发生,印度政府加强了信息安全措施,特别是出台法律规定商业和个人使用的加密技术中密钥长度不得超过40比特。这虽然有利于政府打击犯罪,但不利于维护个人信息和隐私,将会产生个人网络安全的黑洞。

[65]例如,苹果公司CEO库克公开表示,这将会"攻击它自己的用户,破坏几十年来保护它的用户(包括数千万美国公民)免受……黑客和网络罪犯攻击的安全保障措施。……具有讽刺意味的是,同样一批工程师,把加密程序植入iPhone保护我们的用户,又被责令削弱那些保护,使我们的用户更不安全"。Tim Cook, A Message to Our Customers, Apple(Feb. 16, 2016), http://www.apple.com/customer-letter/.其他互联网公司(如亚马逊、微软、脸书、谷歌等)也联名提交了"法院之友"意见书,明确反对此项举措。See Amicus Briefs in Support of Apple, Apple: Newsroom(Mar. 2, 2016),https://www.apple.com/newsroom/2016/03/03Amicus-Briefs-in-Support-of-Apple/.

[66]参见《澳大利亚新颁布反加密法引起轩然大波》,载白帽汇安全研究院,https://nosec.org/home/detail/2043.html,2020年2月9日访问。

[67] See Kaveh Waddell, How Much Is Encryption Worth to the Economy?, The Atlantic(Nov. 9, 2015), https://www.theatlantic.com/politicstarchive/2015/11/how- much- is- encryption-worth-to-the-economy/458466("The tech industry, however, argues that consumers want better security and privacy and that a weaker encryption standard would be a huge economic hit to U.S. companies, because consumers would shift to apps and services with strong encryption made overseas.").

[68]参见《〈密码法〉元年到来王小云院士郑州专题演讲密码应用与区块链》,载大河网,https://news.dahe.cn/2020/01-19/581135.html。

[69]美国国安局曾经被揭露在密码技术中植入后门;荷兰政府则在2016年表示不会强迫密码公司留后门。参见同前注[55],左亦鲁文,第155页。

[70]技术界人士已经有此提议。参见链证经济:《高承实博士:密钥托管是区块链项目落地的必要妥协》,载简书网2018年11月29日,https://www.jianshu.com/p/d0494b951b81。

[71]参见马民虎、果园、马宁:《自解密义务的法律困惑及其本土适用》,载《苏州大学学报(哲学社会科学版)》2016年第1期,第89-94页。

[72]参见《刑事诉讼法》(2018年修正)第52条规定:"审判人员、检察人员、侦查人员必须依照法定程序,收集能够证实犯罪嫌疑人、被告人有罪或者无罪、犯罪情节轻重的各种证据。严禁刑讯逼供和以威胁、引诱、欺骗以及其他非法方法收集证据,不得强迫任何人证实自己有罪。"

[73]参见同前注[71],马民虎、果园、马宁文,第93页。

[74]See Cynthia Lee, Reasonableness with Teeth: The Future of Fourth Amendment Reasonableness Analysis, 81 Mississippi Law Journal 1133(2012).

[75]崔聪聪、李欲晓、韩松:《〈网络安全法(草案二次审议稿)〉第27条修改建议——以网络服务提供者协助解密义务为中心》,载《中国工程科学》2016年第6期,第36页。

[76]《个人信息保护法》第34条规定:"国家机关为履行法定职责处理个人信息,应当依照法律、行政法规规定的权限、程序进行,不得超出履行法定职责所必需的范围和限度。"

[77]参见王志刚、杨敏:《论网络服务提供者的侦查协助义务》,载《重庆邮电大学学报(社会科学版)》2019年第4期,第25-33页。

[78]参见《个人信息保护法》第35条:"国家机关为履行法定职责处理个人信息,应当依照本法规定履行告知义务;有本法第十八条第一款规定的情形,或者告知将妨碍国家机关履行法定职责的除外。"

[79][美]劳伦斯·莱斯格:《代码:塑造网络空间的法律》,李旭译,中信出版社2004年版,第6页。