**全民国家安全教育之密码法治宣传教育**

2020年4月15日是《中华人民共和国密码法》颁布实施后的第一个全民国家安全教育日。密码安全事关国家安全，密码法是我国国家安全法律制度体系的重要组成部分。

《中华人民共和国密码法》2020年1月1日正式进入实施阶段。

法律意义上的密码和生活中所说的密码有什么区别，又如何分类。这部听上去有些神秘的法律，究竟包含哪些内容，怎样与我们的社会生活息息相关。

国家密码管理局新闻发言人李国海用两集的时间为大家进行解读，上集为《保护国家秘密的密码》，下集为《百姓身边的密码》。

《密码法》解读（上）

——保护国家秘密的密码



观众朋友大家好，欢迎收看《法律讲堂》。从今天起，我将用两期的时间和大家一起讨论《密码法》。

2019年10月26日，十三届全国人大常委会第十四次会议通过《中华人民共和国密码法》，习近平主席签署第35号主席令予以公布，将于2020年1月1日起正式施行。密码法的颁布实施，是我国密码发展史上具有里程碑意义的大事，有助于提升我国密码工作的规范化、科学化、法治化水平，对维护我国网络空间安全、促进信息化发展具有重要意义，也直接关系企业商业秘密的依法保护，关系社会公众在网络空间生活的安全和便利。

有的观众朋友可能要问，我们每天在网上登录电子邮箱，到银行自动取款机上取钱转账时，都提示要输入一串“密码”，密码法就是管这些“密码”吗？今天，我们就先来聊聊什么是密码，为什么要制定密码法。



密码法第2条对密码作了明确的定义，说“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”。



这个定义包含了4层含义:

一是密码的主要表现形式是技术、产品和服务；

二是密码的主要功能是加密保护、安全认证；

三是密码保护的对象是信息等相关内容；

四是密码的本质属性是特定变换的方法。

我觉得在这4层含义中，我们重点要理解的是密码的主要功能和本质属性，也就是说，要明白什么是加密保护，什么是安全认证，又怎么采用特定变换的方法来实现加密保护、安全认证。

加密保护

很容易理解，就是将明文变成密文。通俗地讲，就是将原来大家都看得懂的信息，能够识读的文字、能够观看的视频，变成一堆完全看不懂的数字或符号。举个简单的例子，小张约小王去食堂吃饭，但是不想让别人知道，相互约定以“0”代表小张，“1”代表小王，“7”代表食堂，“9”代表吃饭，“0179”就代表了“小张约小王去食堂吃饭”的意思，这就达到了保护信息的目的。

人类使用密码的历史非常久远，在古代就用密码传递秘密军事情报。我国有文字记录的密码使用历史，可以追溯到三千多年前的周朝。据《太公六韬》记载，姜子牙发明了一种利用鱼竿长短传递战场信息的方法，也就是将鱼竿制成不同长短的数节，不同的长度代表不同的含义，一尺长的鱼竿代表战争取得大胜；9寸代表破阵擒将；最短的3寸代表失利亡土。这种加密技术不使用一个文字，即使被截获也不会泄密。现代战争，更是将密码运用到了极致，战场上所有指令的下达、情报的传递都要进行加密保护。二战中的著名战役——中途岛决战，生动展现了密码在战争中决定胜负的关键作用，珍珠港事件后的6个月间，日军占尽上风，美军太平洋舰队节节败退。但美军舰队是如何在中途岛战役得胜，并以此扭转太平洋战争劣势的呢？就是因为1942年3月，美军密码破译人员经过不懈的努力，终于破解了日军的JN-45密码，提前察觉日军已锁定中途岛，并利用情报优势将日军引入陷阱。

安全认证

安全认证，就是通过特定变换，确认信息是否被篡改、是否来自可靠的信息源以及确认行为是否真实。举个网上银行转账的例子。你在早上6点整向银行申请给朋友的账户转一万块钱。但银行怎么确认这个申请是你本人真实意思，确认转账金额分毫不差呢？这就需要安全认证。在不使用密码产品的情况下，你在网上输入的姓名、银行卡号、身份证号、银行卡口令等各种信息，极易被不法分子获取，接下来，不法分子就可以用这些获取的信息，假冒你的名义从你的银行卡里转钱了。为确保网上银行交易的安全，银行为我们办理的U盾或动态令牌就是用于安全认证的密码产品。

以动态令牌为例，你输完转账信息后，银行的信息系统会要求你输入令牌里的6位或8位数字。这几位数字是怎么来的呢，这是使用特定密码算法，根据你的身份、账号、金额、申请时间等信息计算出来的。这个过程中，只要任何一项信息变化，比如转账金额变为9999块，或者转账时间变为6点零1分，都会使令牌显示的数字完全不同。这样就通过动态令牌的认证保证了你网上银行交易的安全。

通过密码法给出的密码定义，以及上面几个例子，大家应该明白，我们输入的取款密码、网站的登录密码，实际上并不是密码法中规定的“密码”，准确讲应该称为“口令”，只是一种最简单、最初级的认证方式。而真正的密码，藏在安全支付设备中、藏在网络系统内，默默守护国家秘密信息安全、守护我们每个人的信息安全。它既熟悉又陌生，既遍布各处又蒙着神秘的面纱。神秘的密码也经常成为引人入胜的影视题材，上世纪50年代放映的《永不消逝的电波》，坚贞不屈的密码工作者李侠的形象深深地印刻在人们的脑海中。近些年的《风声》《暗算》等影视作品，也为我们讲述了一个个关于密码、密码工作者的动人故事，很多人看了以后，都被他们的聪明才智和对党和国家的绝对忠诚深深打动。

认识了密码，就能充分理解我国颁布实施《密码法》的重大意义。

从法治建设上讲，这是构建国家安全法律制度体系的重要举措。

经历了近90年的历程，密码工作从无到有，从弱到强，逐步发展壮大，一直是我们党对敌斗争的重要战场，是保证国家安全和根本利益的重要防线，也是党中央、国务院、中央军委实施领导指挥的重要渠道，直接关系着国家的政治安全、经济安全、国防安全和信息安全。

长期以来，我国密码领域只有一部行政法规——《商用密码管理条例》，无论是立法位阶还是法律效力，都不能完全适应新时代密码事业发展的需要。制定《密码法》，就是要把党对密码工作的最新要求通过法定程序转化为国家意志，把密码工作的各个重要环节和关键要素纳入法治轨道。

《密码法》是我国密码领域第一部综合性、基础性法律，它将与《国家安全法》《网络安全法》《反恐怖主义法》《反间谍法》等等一起，共同构成国家安全法律制度体系，以法的名义护卫国家安全。

从国家战略上讲，这是维护国家网络空间主权安全的重要举措。

当今世界，信息技术日新月异，网络安全作为国家安全的重要组成部分，深刻影响传统领域国家安全，深刻影响国家长治久安和经济社会发展，关系人民群众福祉。在保障网络安全的各种手段和技术中，密码是目前世界上公认的最有效、最可靠、最经济的关键核心技术。在网络世界，密码就像一个看不见的卫士，已经渗透到社会生产生活的各个方面。



从涉及国家安全的保密通信、军事指挥，到涉及国民经济的金融交易、防伪税控，再到涉及公民权益的电子支付、网上办事等等，密码都在背后发挥着基础支撑作用，维护着国家网络空间的主权、安全和发展，所以有人形象地说，“密码是网络安全的DNA”。

制定和实施密码法，就是要规范密码管理，引导全社会合规、正确、有效地使用密码，让密码在网络空间更加主动、更加充分地发挥保障作用，构建起以密码技术为核心、多种技术交叉融合的网络空间新安全体制。

从密码自身发展来讲，这是推动密码事业高质量发展的重要举措。

党的十八大以来，密码事业取得了历史性成就，实现了历史性变革。特别是随着网络强国战略、国家信息化发展战略、国家大数据战略等的实施，我国密码事业加速转型升级，如今，密码的作用已经不再是单一的信息加密了，还可以用于身份识别、安全隔离、完整性保护等。密码的应用领域也极大拓展，不再是原来的仅仅服务于党政军领导机关和机密要害部门，而是已经“飞入寻常百姓家”。

制定和实施密码法，就是要积极推进密码领域职能转变，进一步推进“放管服”改革，建立健全密码法治的实施、监督和保障体系，使密码更好地为党和国家工作大局服务，更好地为广大人民群众的生产生活服务。



通过刚才的讲述，我们了解了什么是密码，也认识到了密码作为党和国家重要战略资源的重要性。那么这么重要的战略资源，在我国的领导和管理体制是什么？又是怎么实施管理的呢？

我国密码管理体制

密码法第四条明确规定，坚持中国共产党对密码工作的领导,这一句强调了党管密码的根本原则。党管密码，是密码工作的优良传统，也是密码工作的灵魂。我党密码工作是毛泽东、周恩来等老一辈无产阶级革命家亲手创建的，一直在党的领导下发展壮大。密码法同时明确了中央密码工作领导机构对全国密码工作的统一领导地位，并在第五条明确了分级负责的管理体制：“国家密码管理部门负责管理全国的密码工作。县级以上地方各级密码管理部门负责管理本行政区域的密码工作。国家机关和涉及密码工作的单位在其职责范围内负责本机关、本单位或者本系统的密码工作”。



这就意味着，在党管密码的根本原则指导下，建立国家、省、市、县四级密码管理体制。具体来说，就是国家以及省、市、县各级密码管理局承担着管理我国密码工作的重任。除此之外，还有一些国家机关和涉及密码工作的单位在其职责范围内负责本机关、本单位或者本系统的密码工作。



为了对密码实施科学管理，确保密码安全保密，充分发挥密码在保护网络与信息安全中的核心支撑作用，密码法按照保护信息的不同，将密码分为三类，分别是核心密码、普通密码和商用密码。

核心密码和普通密码

用于保护国家绝密级、机密级、秘密级信息，普通密码用于保护国家机密级、秘密级信息。何时使用核心密码，何时使用普通密码，要依据信息使用的主体、秘密信息的性质以及具体的使用场合来确定，在这方面密码法都有明确的规定。

商用密码

用于保护不属于国家秘密的信息，公民、法人和其他组织都可以依法使用商用密码。对密码实行分类管理，是党中央确定的密码管理根本原则，是保障密码安全的基本策略，也是长期以来密码编制和应用工作经验的科学总结。

接下来的时间，我们聊聊“神秘”的核心密码和普通密码。它们的诞生可以追溯到上个世纪三十年代。当时，党和军队的秘密通信基本采用鸡毛信这种人工的原始传递方式，时效性、安全性都比较差，一封信从上海党中央到中央苏区来回就要两个多月。特别是大革命失败后，革命形势急转直下，党中央急需一种秘密高效的通信方式。在这种紧急情势下，老一辈无产阶级革命家创建了中国的密码事业，为中国革命胜利做出了不可磨灭的贡献。党中央委派周恩来同志亲自领导创建党的密码通信渠道。

1930年1月15日夜里，一道红色无线电波划破了漆黑的夜空，在上海党中央和香港南方局之间传递着秘密信息，这一天，被载入了中国革命的史册，我国的密码事业也从此诞生。90年来，伴随着党和国家革命、建设、改革的各个历史时期，密码事业在治党、治国、治军，内政、国防、外交方面都发挥了极其重要的作用。

《长征组歌》中有一句歌词，说“毛主席用兵真如神”。那么是什么支持毛主席作战，使他用兵如此之神呢？是密码，是密码通信，为毛主席指挥作战提供了“千里眼”和“顺风耳”。当时的红军不仅使用密码电台进行秘密通信，还利用他们的聪明才智，破译了国民党部队的重要密码。

1935年3月28日，红军四渡赤水期间，中央红军进抵乌江北岸沙土、安底地区。3月30日，军委二局获悉敌中央军周浑元、吴奇伟两路纵队主力也向乌江北岸前进。周浑元、吴奇伟部队是蒋介石的嫡系部队，也是蒋介石围剿中央红军的主力部队之一。与这两只劲旅在乌江北岸遭遇，必将对红军造成一场极为不利的血战！在这千钧一发之际，红军的密码通信人员利用掌握的敌方密码和电文格式，冒充督战的蒋介石，令周浑元、吴奇伟两部向西前进。通过巧妙的“调虎离山”，中央红军争取到了宝贵的一天时间，于3月31日南渡乌江，跳出了敌人的合围圈，将几十万敌军远远地甩在身后，又一次巧妙地躲过了敌人的围追堵截。

在三大战役期间，毛主席亲自起草密码电报就有197份，批签的密码电报多达上千份，通过这些电报，高效快捷地指挥着军事作战，直接领导到军团一级，实现了“最小的指挥部，指挥了世界上最大的战争”这样的神话。周恩来同志曾风趣地说：“我们这个指挥部，一不发枪，二不发粮，只发电报，就把国民党打败了。”

密码不仅在革命战争年代作用突出，和平时期，也同样是党中央、国务院，以及各级党委和政府实施领导指挥的特殊法宝和重要渠道。特别是在党和国家的重大活动，以及抗洪抢险、抗震救灾等突发事件中，密码通信的作用更加凸显。密码电报有着无声的力量，它代表着中央的指示和政令，代表着党委政府的决策和指挥，对统一思想、凝聚力量、增强信心，起着不可替代的重要作用。革命战争时期，连通了密码电报就找到了组织，和平年代，在危难险阻之中，收到了密码电报，就意味着得到了胜利的指引。

2008年5月12日，汶川发生特大地震，北川、汶川县城与外界失去了一切联系，一时成为了孤城。震后72小时是抢救的黄金时间，我们的密码干部临危受命，冒着生命危险，乘坐直升飞机第一时间赶赴现场，迅速在废墟上建立起密码通信，第一时间向党中央报告了灾情，为党中央决策指挥提供了第一手宝贵信息。党中央、国务院抗震救灾的指示政令，也及时准确地传送到灾区，为确保人民群众生命财产安全做出了重大贡献。

可以说，核心密码、普通密码伴随着军事斗争一路走来，演绎出一幕幕跌宕起伏的攻防对抗传奇，也逐渐奠定了密码作为党和国家“命门”“命脉”的重要地位和作用。制定和实施密码法，对于全面提升密码工作法治化和现代化水平，加强核心密码、普通密码管理，具有十分重要的意义。同时，由于核心密码、普通密码本身属于国家秘密，密码法规定了核心密码、普通密码的管理原则、使用制度、安全管理制度、监督检查制度和工作保障制度。

刚才为您讲述了核心密码和普通密码，而密码除了用于保护国家秘密，也与我们老百姓的生活息息相关。那么，密码在我们的日常生活中都有哪些应用？密码法又是怎么规定的呢？我们将在明天的节目中继续为您讲述。

今天的法律讲堂就到这里，谢谢大家的收看，再见！

《密码法》解读（下）

——百姓身边的密码



各位观众朋友大家好！欢迎继续收看密码法解读的第二讲——“百姓身边的密码”。

上期，我们给大家讲了什么是密码，为什么制定密码法，以及三类密码中涉及国家秘密的核心密码、普通密码。下面，我将给大家介绍一下我们身边的密码，也就是商用密码。

早晨醒来，你拿起手机输入口令，手机的口令就是用商用密码进行加密保护，并储存在通过安全认证才能正确访问的手机特殊存储区域。

我们出行，飞机票、火车票都通过网络购买，在线支付的全过程都有商用密码的保护，第二代居民身份证也是通过商用密码保证人证一致，帮助你顺利通过检票乘车，列车行进过程中，密码始终在为列车的安全运行和控制调度提供保障。



工作中，网上办公、网上办事、交税纳税，后面都有商用密码在默默贡献。可以说，商用密码总是如影随形，保障着你工作生活中的网络和信息安全，但是你基本感觉不到它的存在。

在密码法中，商用密码是这样定义的：“商用密码用于保护不属于国家秘密的信息。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。”虽然商用密码用于保护不属于国家秘密的信息，但是如果认为，不属于国家秘密的信息就不需要密码保护，用于保护不属于国家秘密信息的商用密码就不重要，那就完全误解了网络安全，误解了商用密码。实际上，网络空间处处用到商用密码，商用密码在维护国家安全、促进经济社会发展、保护人民群众利益方面发挥着重要的作用。

商用密码的应用同样有着悠久的历史。

清朝末年，山西平遥城内有个靠乞讨为生的老太太，拿着一张1200两的白银汇票，到中国最早的票号日昇昌兑付白银。这张汇票已时过三十余年，经查验无误，实现了兑付。山西票号百年历史上，没有发生过一张假汇票，这也是票号之所以能“一纸汇通天下”的最有力的保证。那么，山西票号是如何防止造假的呢？

在当时的条件下，由于技术问题，银票的防伪是十分困难的。为此，山西票号创造了一套汉字密码，用于银票防伪，即在正常的票据下面会写上一行字，别人看不懂，其实是银票对应的日期和数目，如果和银票上正常的数目和存款日期一致，就是真的；如果不一致，就是假的。而真假的辨认，只有掌握密码的人才能做到。

日昇昌在平遥古城旧址柜房的侧墙上，挂着一幅诗文。诗文写到：“谨防假票冒取，勿忘细视书章”、“堪笑世情薄，天道最公平，昧心图自利，阴谋害他人，善恶总有报，到头必分明”、“赵氏连城璧，由来天下传”以及“国宝流通”……。看上去，这些诗文好像是票号的工作守则，其实不然，它是中国最早的银行密押制度，即用汉字代表数字的密码。诗文的第一部分，共两句、12个字，对应的是每年的12个月份；诗文的第二部分，共6句、30个字，对应的是每个月的30天；诗文的第三部分，共2句、10个字，对应的是数字壹到拾，用于记录银两数目；诗文的最后一部分，4个字，对应的是银两的计量单位“万千百两”。

更为关键的是，这些密押也不是一成不变，用过一段时间，会进行变更，如果有人想要破译或者伪造，更是难上加难。这就是历史上的“商用密码”。

进入现代社会，商用密码的应用范围越来越广。

电信、电力、能源、金融、交通等国家关键信息基础设施，我们日常用到的刷卡消费、社保系统、电子邮件，都大量使用商用密码，用来实现网络和信息的加密保护和安全认证，商用密码技术和手段也越来越先进。

先说说刷卡消费。当我们利用银行卡刷卡消费时，先在商家POS机上刷卡，输入银行卡口令后，POS机会将此次交易的口令等信息加密，与银行后台数据库中的个人账户信息进行核对，确认持卡人是真实的，然后基于消费信息、流水号、金额等，使用密码技术计算出一串用于安全认证的数字，用密码术语讲就是交易信息的“数字签名”，通过网络传输给银行后台系统，后台收到信息及其数字签名后，会再用密码技术验证这个签名与发来的消费信息、金额等是否一致，核对通过后反馈交易成功。交易成功后，银行会将对应的金额从持卡人账户转到商家账户，交易完成。整个交易过程，利用密码技术，实现了“交易双方的身份真实有效”、“交易的账号、口令不被第三方非法获取”，“交易金额不被篡改”，“交易双方的行为事后不能抵赖”。

再看看发票防伪。1994年我国开始使用增值税发票，由于当时发票只采用了类似人民币物理防伪的方法，出现了不法分子开具假票、大头小尾，也就是阴阳票等偷逃国家税款的行为，造成国家税款的大量流失。为此国家组织有关部门研制了增值税防伪税控系统。增值税防伪税控系统采用商用密码技术保护涉税信息，增值税发票上的所有票面信息都要经密码进行加密，产生密文，这一长串乱码以四个二维码的形式打印在发票右侧的密码区。在税额抵扣环节对密文进行解密，解密后的发票要素与发票明文进行比对，从而确定发票的明文信息是否真实。如果比对后没有通过，就可以认定是假发票，税额不能抵扣。这一防伪技术每年为国家减少税收流失1000亿元以上。

接下来聊聊最近备受关注的“区块链”。2019年10月24日下午，中央政治局就区块链技术发展现状和趋势进行第十八次集体学习，习近平总书记对加强区块链技术研究、发展区块链应用产业作出重要指示。那什么是区块链呢？通俗的说，区块链是一种由多方共同维护，利用密码技术实现数据难以篡改、防止抵赖的分布式账本技术。大家有没有觉得“难以篡改”“防止抵赖”这些词似曾相识？对！这些功能就是利用密码技术实现的。所以说，区块链最核心的技术就是密码，正是因为有了密码，区块链上的数据才能做到完整有效，从而构建网络信任机制。

通过这几个例子，我们应该对商用密码的重要作用有了更为准确全面的认识。党中央高度重视商用密码发展，1993年，就作出了大力发展商用密码的决定；1996年，中央政治局常委会议专题研究我国商用密码发展问题，并作出了加强商用密码管理的重大决策；1999年，国务院颁布《商用密码管理条例》，将党中央、国务院关于商用密码工作的一系列方针、政策和原则以国家行政法规的形式确定下来；2002年，商用密码管理办公室成立；2005年，国家密码管理局正式成立。

这一系列战略举措，推动了商用密码的健康发展，更好地服务国家安全和人民社会生活。党的十八大以来，在以习近平同志为核心的党中央坚强领导下，我国商用密码进入了发展的快车道，密码科研和产业全面推进，商用密码应用的广度和深度大幅提升。

观众朋友们，商用密码在维护国家安全、促进经济社会发展、保障人民群众利益方面有如此重要的作用，密码法关于商用密码的发展和管理都作出了哪些规定呢？

按照党管密码原则和简政放权的要求，密码法在商用密码科技创新、产业发展、人才培养、教育培训、标准化、检测认证、密码应用、进出口、电子认证、行业自律、监督管理等方面作出相应规定。

下面，我们一起来了解一下商用密码的具体管理规定。

1 鼓励、促进商用密码技术和产业发展

大家都知道，随着信息技术，特别是5G、人工智能、大数据等产业变革性技术的快速发展，人们生活已经与网络深度融合，在网络空间有大量的个人隐私和信息安全亟需保护，密码作为保障网络空间安全的核心技术和基础支撑，发挥着越来越重要的作用。经过20多年的发展，我国商用密码产业已初具规模。金融数据密码机、ATM、POS终端设备、金融IC卡等，在保护国家金融关键信息基础设施，保护人民群众的财产安全；纵向加密认证网关、智能电表等，保护着国家电网关键信息基础设施，保证着人民群众的用电安全；居民二代身份证、移动警务、加密摄像头等，在维护社会公共秩序，保护人民群众财产和人身安全方面发挥着重要作用；加密通信手机，为企业、公民个人保护信息安全提供了便捷工具；智慧城市、智能家居，也都以商用密码作为基础支撑。可以说，商用密码产品已渗透到我们日常生活的方方面面。

据不完全统计，2018年，商用密码产品销售总额近300亿元，与未来的市场需求相比，还有很大的发展空间。密码法第21条明确规定，“国家鼓励商用密码技术的研究开发、学术交流、成果转化和推广应用，健全统一、开放、竞争、有序的商用密码市场体系，鼓励和促进商用密码产业发展。”就是要进一步激发各类市场主体活力和社会创造力，努力为商用密码科技创新、产业发展营造更好环境，满足全社会的应用需求。

2 遵循国际规则开展国际交流与合作

我们始终鼓励和支持我国商用密码企业走出去，服务更多的国家和地区；同时，也欢迎外商投资企业在中国依法开展商用密码业务。我国自主设计的祖冲之（ZUC）序列密码算法、SM2/SM9数字签名算法、SM3杂凑密码算法等商用密码算法已经成为国际标准，标志着我国商用密码理论研究及算法设计达到国际一流水平，同时，我国密码产品和技术积极服务“一带一路”建设，已出口10多个国家和地区，为维护国际信息安全贡献了中国力量。

对密码领域的国际交流与合作，《密码法》有明确规定，要求坚持非歧视原则，依法平等对待包括外商投资企业在内的商用密码从业单位，明确商用密码技术合作的前提是基于自愿原则和商业规则，行政机关不得要求强制转让商用密码技术。这些条款，回应了外商投资企业对知识产权保护问题的关切，充分表明了我们对商用密码知识产权保护的决心，展现了我国在商用密码领域开放自信的态度。

3 加强标准引领，推进商用密码检测认证体系建设

实施检测认证制度是保障产品质量的国际通行做法，密码法从激发市场活力，促进密码产业发展的角度，重塑了现有的商用密码产品管理体系，由单一的准入许可调整为多样化检测认证。正如大家熟悉的手机检测一样，一款新手机进入市场销售前，首先需要先通过入网检测，以确认能在移动网络中正常使用，商用密码产品和服务上市前，也需要通过严格的检测认证。密码法规定，商用密码产品和服务以自愿检测认证为主，给了生产单位更多的选择空间。同时，又对特定范围内的商用密码产品实行强制性检测认证，把好质量关，确保不出安全问题。这种做法既充分考虑与《网络安全法》等相关制度相衔接，共同维护国家安全和社会公共利益，也充分尊重市场需要，符合世贸组织（WTO）规则。

国家密码管理局一直高度重视商用密码标准化工作，目前，已发布商用密码国家标准29项，行业标准91项，覆盖商用密码技术、产品、服务、应用、检测和管理等全范围，建立了较为齐全完备的商用密码标准体系，为建立检测认证制度、规范市场管理提供重要的标准化依据。

4 强化对商用密码应用的管理

商用密码是把“双刃剑”，用得好会造福社会，如果被坏人利用，则危害无穷。例如，2017年5月，一款名为“魔哭”（Wanna Cry)的蠕虫勒索软件袭击全球网络。该勒索软件影响全球150多个国家和地区，超过30多万台设备受到感染。这种病毒就是利用密码技术，对受害者电脑内的重要文件进行加密，再胁迫受害者通过比特币支付赎金。因此，密码法从两方面对商用密码使用作出明确规定。

一方面，该用密码的必须依法依规使用。密码法规定，“法律、行政法规和国家有关规定要求使用商用密码进行保护的关键信息基础设施，其运营者应当使用商用密码进行保护，自行或者委托商用密码检测机构开展商用密码应用安全性评估”。

另一方面，密码不能随意滥用。密码法规定，任何组织和个人不得利用密码从事危害国家安全、社会公众利益、他人合法权益等违法犯罪活动。任何组织或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。

5 实施商用密码进口许可和出口管制

刚才我们已经提到密码是把“双刃剑”，既可以用于合法的信息保护，也可以被用来从事违法犯罪活动，具有一定的特殊性，对其实行进口许可和出口管制，是履行国际义务、维护国家安全和社会公共利益的必要手段，符合世贸组织规则和我国对外贸易法的规定，也是国际通行做法。同时，为避免进口许可和出口管制对正常贸易造成不必要的影响，密码法明确界定了进口许可、出口管制的适用条件，并通过制定清单，明确界定管理范围。

密码的进出口许可，不会影响正常贸易，也不会影响社会公众的日常生活。密码法规定对于大众消费类产品所采用的商用密码不实行进口许可和出口管制制度，也就是说我们社会公众通过常规零售渠道购买的，只供个人使用的，对国家安全、社会公共利益带来的风险较小且可控的，不在管理范围之内。这充分体现了密码法在保障安全的前提下促进发展的立法思路。

6 强化行业自律和监督管理

商用密码产业与国家网络化、数字化、智能化进程密切相关，必须不断适应形势，创新管理，提升效益。对此，密码法作出了系列规定，强化行业自律和监督管理。

一是重视发挥行业协会等组织的作用。加强行业自律，推动行业诚信建设，促进行业健康发展。

二是构建新的监管体系。监管思路上，从事前审批转到事中事后监督；监管方式上，把日常监管和随机抽查相结合；监管手段上，建立统一的商用密码监管信息平台，推进事中事后监管与社会信用体系相衔接。

三是明确了法律责任。对违反密码法有关规定的行为，明确了相应的罚则，让密码法律制度“长出牙齿”，确保法律有效实施。

《中华人民共和国密码法》的颁布实施，为密码依法管理提供了根本遵循，为密码科学发展提供了法律支撑，为维护网络空间安全提供了法治保障，为密码领域国际交流与合作提供了法律依据，为公民、法人和其他组织维护网络空间合法权益提供了法律武器。2020年是密码法施行元年，也是密码工作创建90周年。我相信，随着《密码法》的颁布实施，通过全社会的共同努力，必将开启密码事业发展的新局面，密码也将在维护国家安全和保障人民群众生产生活中更好地发挥作用。

今天的法律讲堂就到这里，谢谢大家的收看，再见。

《焦点访谈》播出密码法专题节目——《守护安全，密码在你身边》，也让我们一同学习吧~~~

（来源：国家密码安全局微信公众平台）(转载自网络，如有侵权请联系我们删除。）