

关于《密码法》 你了解多少？

目录

目录

第一章 密码与密码的法律监管

- 一、密码危机与密码法需要考虑的那些事
- 二、密码的技术和法律定义：哪些是密码，哪些不算
- 三、密码的法律监管机构
- 四、密码的法律分类

第二章 密码保护国家秘密

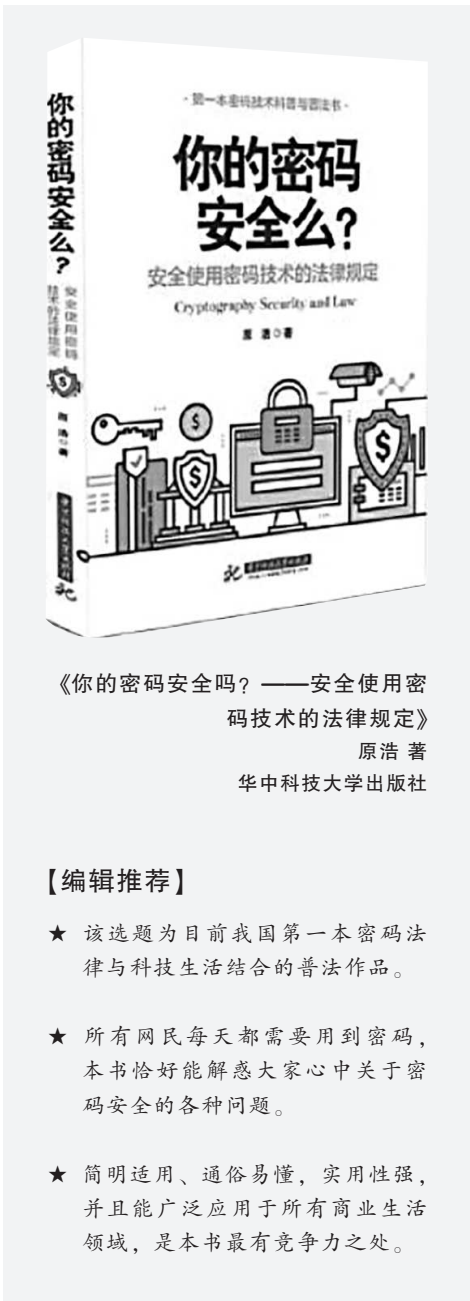
- 一、涉及国家秘密保护的核心密码、普通密码及其基础性作用
- 二、密码工作机构对密码的保密管理
- 三、密码管理部门对密码工作机构的监督检查

第三章 商用密码

- 一、商用密码和商用密码市场
- 二、商用密码标准
- 三、商用密码检测认证的一般规定
- 四、强制检测认证

第四章 密码违法行为的行政和刑事法律责任

- 一、窃取他人保密信息或侵入他人密码系统的法律后果
 - 二、非法使用核心密码、普通密码的法律责任
 - 三、与密码检测认证有关的法律责任
 - 四、与“密评”相关的法律责任
- (略)



《你的密码安全吗？——安全使用密码技术的法律规定》
原浩 著
华中科技大学出版社

【编辑推荐】

- ★ 该选题为目前我国第一本密码法律与科技生活结合的普法作品。
- ★ 所有网民每天都需要用到密码，本书恰好能解惑大家心中关于密码安全的各种问题。
- ★ 简明适用、通俗易懂，实用性强，并且能广泛应用于所有商业生活领域，是本书最有竞争力之处。

【内容简介】

本书从法律、科技与民众生活的角度，采用通俗易懂、问题明确、实务操作性强的内容撰写方式解读密码，从社交软件到在线交易、从智能终端到智慧城市无处不在。这种深度渗透中看到：其正在成为包括中国近十亿网民在内的信息技术和网络空间活动的“基本配置”，对密码产品、服务的技术关注和需求已经超越了从普及到专业的所有方

【作者简介】

原浩，中华全国律师协会网络与高新技术法律专业委员会研讨员、中国信息安全法律大会专家委员会副秘书长委员，江苏省信息网络安全协会法律专家。合译有《软件开发生命周期》（微软），参编或著有

【精彩节选】

随着计算机和各种智能设备的存储、处理能力增强和成本降低，通过加密等复杂计算方式保护数据的做法得到普及，而对个人信息和隐私保护意识的提升，也使公众迫切需要通过加密等方式获得安全感。有研究发现，2019 年互联网中有 87% 的信息使用了不同的加密方式以防止第三方访问和获取。

通过选择可用的加密保护方式，企业和个人可以有效地保护商业秘密、个人隐私等敏感数据。例如，企业通过具有加密功能的存储设备（加密硬盘、移动设备）对存储的数据进行加密，只有经过身份验证的人员才能访问该信息，即使设备失窃，也可以部分消除数据泄露的忧虑。再如，目前包括购物、邮箱，甚至车票订购等在内的众多在线服务已经开始对平台上的通信进行加密。例如，在访问网络地址时，我们会发现早期默认的 http 开头已经悄然升级到了 https，这个“s”即表示增加了传输层加密协议 SSL，其中内容仅会会话参与者可用。对于智能终端，比如手机设备中的即时通信工具（或者称之为“社交软件”），实现端到端加密（E2EE）已经成为应用程序开发者推崇的“噱头”。

加密技术的广泛应用虽然提高了个人和企业保护各类非公开信息的安全性，但同时也给执法机构维护社会公共安全乃至国家安全带来挑战。例如，2017 年，众所周知的勒索软件“Wannacry”通过加密用户计算机的特定类型数据，威胁用户在指定时间内支付比特币“赎回”数据，众多个人用户和公共服务深受其害。再如，无法登录或访问某些设备或应用，执法机构难以提取犯罪嫌疑人智能手机上的数据。甚至在 20 世纪 90 年

代，美国发生了围绕密码进出口的所谓“第一次密码战争”。

密码技术如此关键，早在 1997 年，发达国家“俱乐部”——经合组织就发布了《密码政策指南的建议》。该建议认为，密码技术对于全球信息通信网络技术和电子商务的发展都至关重要，应当尊重国家密码政策、立法的执行，并应当通过密码应用保护各方基本权利，包括通信安全和个人数据保护，应考虑在“促进密码使用的同时不会危害公共安全、执法和国家安全”。建议的指南部分明确了各国在国家层面确立密码政策应当遵循的八项基本原则，包括依法有权使用密码技术、市场驱动密码发展、隐私和个人数据保护等。因此，密码技术和应用牵涉到包括国家、公众、企业和个人在内的各种主体的权利义务，《密码法》正是为安排和协调这些不同，甚至相互冲突的利益与诉求而生的。

《中国律师业务报告（2015）》（电子商务部分）、《网络安全法适用指南》《互联网内容安全管理》《中国网络安全法治研究：合规卷》等，部分论文发表或入选于《信息网络与高新技术法律前沿》《涉外案例精选》等。

《密码法》的立法定位并未局限于既有密码技术、产品，而是通过对密码活动主体、密码服务的弹性扩充实现对前沿密码问题的规范和调整。面对未来，密码问题大概如下：

(1) 基于云计算的服务，端到端加密的使用范围不断扩大，不仅可以保护传输中的数据，即时通讯工具的端到端信息加密，或者邮件的端到端内容加密，还可以确保存储在云端的数据得到保护，在此情况下任何第三方（甚至云服务提供商）都无法访问。在这种情况下，法律所面临的主要问题是，社交软件开发、云服务提供商不持有密钥，是否还具有相应的解密能力，是否还应当向执法机构履行协助解密的义务。

《从技术到规则：数字文明的法治进路》



本书分为四个部分。“网络时代的社会秩序”围绕互联网、大数据、人工智能技术的兴起，探究网络犯罪的治理模式、政府的功能转型等社会治理问题；“网络时代的数据保护”围绕大数据在具体领域使用的法律困境；“网络犯罪的证明与证据”针对网络犯罪特点，探讨网络犯罪证明难题的新思路与新方法……

高艳东 连斌 编
浙江大学出版社

《高校网络舆情管理》



本著作系统厘定了网络舆情的相关概念，并基于公共危机管理提出了高校网络舆情应对的原则、方法和路径，并通过不断分析和细化相关案例，借鉴各类媒体环境下应对舆情的有效经验，提高高校对于网络舆情的认知，梳理总结出多种可行的应对路径；同时，本著作也指出了面对纷繁复杂的网络信息……

李宝琴 著
中国政法大学出版社

《法学方法论》



本书是一部法学理论方面的经典著作。其主要介绍了十九世纪初至一次世界大战结束期间，德国的法学理论及方法论。正如第五版的“法学方法论”，六版也是以节略的“学生版”来发行的。节略的部分是论及历史、批判性部分的前四章，其主要处理十九世纪初到一次大战结束之间，德国的法律理论及方法论。

[德] 卡尔·拉伦茨 著 陈爱娥 译
商务印书馆