DOI 10.15302/J-SSCAE-2016.06.007

# 《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

**崔聪聪[1]，李欲晓[2]，韩松[1]**

（1. 北京邮电大学互联网治理与法律研究中心，北京 100876；2. 中国网络空间安全协会，北京 100010）

**摘要：**网络服务提供者协助解密义务，隐含着公权力（侦查权）与私权利（通信秘密权、隐私权）之间的冲突。用户的非公开信息应该在可控、可追溯基础上，遵循必要性原则和比例原则，综合考虑执法成本，司法机关经由法律确定网络服务提供者履行协助解密义务获取，进而达到社会治理管控、公众安宁生活与网络服务提供者营业自由的综合效益最大化目标，避免落入公权力严重侵犯私权利的情形或者出现政府失效的无序状态。

**关键词：**协助解密义务；必要性原则；比例原则；可控、可追溯；救济措施

**中图分类号：**D922.1　　**文献标识码：**A

# The Obligation of Decryption Assistance by Internet Service Providers: Suggestions on the Amendment of Article 27 of the Network Security Law Draft (Second Draft)

**Cui Congcong[1], Li Yuxiao[2], Han Song[1]**

(1. Institute of Internet Governance and Law, Beijing University of Posts and Telecommunications, Beijing 100876, China;
2. CyberSecarity Association of China, Beijing 100010, China)

**Abstract:** The obligation of decryption assistance by Internet service providers reflects the conflict between public power (the power of investigation) and the right of privacy (the right of communication privacy, private rights). Internet service providers should gather data under encryption by users on the basis of the principles of controllability and traceability, proportionality, and necessity. Providers should consider choosing their path prudently, supervised by strict procedure. Thus, the overall utility of social governance control, the tranquility of private life, and the business interests of Internet service providers can be maximized. Severe violations of private rights and disorderly situations due to governmental failure can be avoided if these suggestions are carried out.

**Key words:** obligation of decryption assistance; principle of necessity; principle of proportionality; principle of controllability and traceability; remedy measures

**收稿日期：**2016-10-12；**修回日期：**2016-10-18

**作者简介：**崔聪聪，北京邮电大学互联网治理与法律研究中心，副主任，副教授，主要研究领域为网络法；E-mail: cuicongcong@bupt.edu.cn

**基金项目：**中国工程院重大咨询项目“网络空间安全战略研究”(2015-ZD-10)

**本刊网址：**www.enginsci.cn

## 一、前言

网络时代，犯罪日趋国际化、组织化、隐蔽化和高科技化。近年来，暴恐分子利用通信加密及存储技术进行传播暴恐音视频、接受境外指令、勾连策划恐怖袭击，从而严重威胁国家安全和社会公共安全。密码技术的泛化利用客观上给司法机关的刑事侦查活动造成障碍，加密技术使大量的危害国家安全和社会公共安全的案件无法及时被发现、制止和惩处。出于保障国家安全、维护社会秩序等诸多目的，侦查机关在侦办刑事案件时，有时不得不要求网络服务提供者协助获取个人处于加密状态的信息。法律有必要明确执法协助的范围及其程序，在保护用户隐私以及国家安全之间寻找一个平衡点，否则执法协助可能沦为某些机关或部门滥用权力、侵害公民人身权利的“通行证”。

## 二、协助解密背后的权利（力）冲突——以苹果解密门为例

### （一）苹果解密门争议焦点及结果

自密码技术民用化以来，技术利用与执法需求的博弈从来没有停止过[1]。密码技术使用的初衷是实现信息的秘密性，为公民的通信秘密权提供技术支撑，但违法行为人同样可以利用密码技术隐匿犯罪事实和证据，因此，密码技术利用产生的执法障碍是始终无法回避的问题。2016 年 2 月 16 日，美国联邦调查局针对加州圣伯纳迪诺赛耶德 · 法鲁克袭击案中获取的 iPhone 手机，经由加州法院发出搜查令要求苹果公司对涉案 iPhone 手机进行协助调查。苹果公司认为美国联邦调查局要求苹果公司在 iPhone 构建后门会破坏其自由以及威胁用户信息安全，并以此为由拒绝协助调查。2 月 28 日，纽约州地区法院受理苹果公司的诉讼。法官 James Orenstein 认为，美国政府对《全令法案》（All Writs Act）的解读过于宽泛，是有违宪法精神的做法，且搜查令中法律引述不当。3 月 7 日，美国司法部要求该法官撤回前判决并命令苹果公司协助解密。3 月 22 日，美国联邦调查局通过以色列 Cellebrite 公司将涉案 iPhone 手机破解。

本案中，由于犯罪嫌疑人已被警方击毙，警方调查陷入僵局。与电信运营商向执法机构提供保存在其服务器内的用户短信行为相比，本案中网络服务提供者的协助义务被放大到解密用户的加密信息，并且主动突破用户协议进行解密，无疑会引发用户对个人信息和隐私安全的担忧。无论是美国联邦调查局援引的《全令法案》，还是苹果公司援引的《美国宪法》第二和第五修正案，事实上都是工业时代的法律。美国联邦调查局要求网络服务提供者的协助执法义务扩大到解密和提供用户端文件，但是，对用户端信息的取证不能简单地类推适用现实的文件夹或者保险箱[2]。如果不对网络服务提供者执法协助义务进行细化，而仅仅出于实用主义目的泛泛规定网络服务提供者应提供力所能及的技术支持，可能引发网络服务提供者的权力泛化以及侦查权力“失控”。如果缺乏程序性保障措施，执法机关和网络服务提供者很容易因滥用权力而侵犯个人隐私和威胁个人信息安全。

### （二）苹果解密门背后隐含的权利（力）冲突

基于保障国家安全、反恐需要而进行的刑事侦查，历来是国家权力与个人权利碰撞最为激烈的领域[3]。依靠网络服务提供者协助解密是国家惩罚犯罪、维护社会秩序的必要手段，是各国在个人自由与控制犯罪之间的抉择。但不可否认，协助解密造成了明显的国家权力、企业营业自由和保护个人尊严、生活安宁等个体根本利益之间的紧张关系。表面上苹果公司拒绝美国联邦调查局解密要求的动机是维护其商业利益，而实质是苹果公司作为公权力与私权利之间冲突的“媒介”，在综合考量各方利益及其影响的基础上做出的价值判断。作为一种预防和控制犯罪的有效手段，协助解密因其具有外溢效应容易侵犯个体的权利而需加以警惕，但是找到一个平衡点并不容易，易言之，在执法的正当需求与企业营业自由、个人隐私保护之间找到适当的平衡点变得越来越困难。

## 三、我国的立法和司法实践

### （一）立法

协助执法是网络服务提供者履行保障网络空间安全义务的重要内容。网络服务提供者作为网络活动最重要的参与者，更应该在数字化执法取证越发困难的网络环境中积极履行协助执法义务。这一义

务要求网络服务提供者为执法机构提供必要的执法便利和技术支持，通常包括通信监控、检查拦截和协助解密等，同时网络服务提供者还应当对协助执法过程中所获取的信息进行保密[4]。

《国家安全法》第七十七条要求公民和组织应当履行维护国家安全的义务，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。《反恐法》第十八条要求电信业务经营者、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。但是，对于其他刑事案件能否要求网络服务提供者协助解密，尚未有相关法律明确确定。《网络安全法（草案二次审议稿）》第 27 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。协助解密作为技术支持和协助的重要组成部分无法可依，甚至对技术支持和协助的范围与程序保障乃至公民权利的救济措施，《网络安全法（草案二次审议稿）》都未明确规定。

### （二）司法实践

与美国令状主义语境的侦查行为管控相比较，我国的立法使得公权力的界限变得模糊，因而需要过多地依靠司法机关的自我约束。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。司法机关在侦查过程中要求运营商提供犯罪嫌疑人的通话记录、短信记录是十分常见的侦查行为[5]。在旧的明文发送情况下按照“一目了然”的侦查原则[6]，可以责令网络服务提供者从服务器中直接提供与案情相关的信息。如今，多数通讯工具或互联网应用已采取密文的发送形式，倘若要求网络服务提供者提供信息，势必要求其强行解密用户信息。

## 四、《网络安全法（草案二次审议稿）》第 27 条修改建议

国家在追诉犯罪中要求网络服务提供者协助解密会侵犯、限制个人隐私权，个人需予以一定程度的容忍，但这并不意味着国家权力在技术侦查中可以不受限制或者制约。对于直接关系到人权的特殊侦查措施，国际通行的做法是通过法律控制来防止权力的无限扩张与滥用[7]。为实现上述目标，《网络安全法（草案二次审议稿）》第 27 条应明确协助解密措施的适用案件种类、适用前提和适用对象。

### （一）适用案件种类

通信秘密权、隐私权以及个人信息控制权均为形成或实现个人人格所不可欠缺的。基于保护公民基本权利的要求，协助解密措施适用的案件范围仅限于重大犯罪案件，包括危害国家安全犯罪、恐怖活动犯罪、黑社会性质的组织犯罪、重大毒品犯罪案件，重大的贪污、贿赂犯罪案件以及利用职权实施的严重侵犯公民人身权利的重大犯罪案件，追捕被通缉或者批准、决定逮捕的在逃的犯罪嫌疑人、被告人的案件，可能判处 10 年以上有期徒刑、无期徒刑和死刑的其他严重危害社会的犯罪案件。“重罪”反映出被害权益的重大性，针对上述犯罪要求网络服务提供者协助解密，足以抵消因侵害公民隐私权、通信秘密权以及企业营业自由而带来的负面影响。贿赂犯罪往往具有隐秘性，侦查机关采用一般侦查措施常常收效甚微，如果不寻求网络服务提供者协助解密，实在难以发现犯罪、调查取证并对违法行为人进行定罪处罚。

### （二）适用前提

协助解密必须在采取一般侦查措施或方式不能或难以查明案情、获取证据、查获犯罪嫌疑人的情况下才可以进行；或者即使有其他方式，但需耗费大量的人力、物力和时间，并可能对个人权利及公共利益造成更大的损害，此即“两害相权取其轻”。必要性原则的另一要义是只有司法机关对个人的行为是否可能造成严重的社会危害结果有了高于合理怀疑的程度，也就是说有实体的证据指向其具有相当程度的社会危害可能，才能要求网络服务提供者协助解密，此时个人的隐私权和通信秘密权应让位于侦查权，经过授权的网络服务提供者协助解密也因此具备实质合法性。

### （三）适用对象

在协助解密过程中，公权力机关想要获取的信息主要有以下两类：行为人的身份信息；犯罪嫌疑人通信的内容。如果将适用对象限制为犯罪嫌疑人

本人，势必导致部分案件由于缺乏犯罪嫌疑人的身份信息而无法要求网络服务提供者协助解密。但如果适用对象没有限制，侦查机关会产生过于充分的“动力”向网络服务提供者索取信息，意图通过海量的信息来筛选出目标证据。在统筹考虑侦查效率与人权保障之间关系的基础上，我们认为协助解密的对象应当是明确且受限的，是与特定的通信线路、电子设备等直接相关的拟制人，不需要适用对象的身份完全明了。此外，作为一种补充侦查的手段，只能在确有必要的情况下，对与被指控人存在密切关联的其他人员实施。

综上，《网络安全法（草案二次审议稿）》第 27 条应该修改为“网络运营者应当为国家安全机关、公安机关和检察机关依法维护国家安全和侦查重大犯罪的活动提供必要的技术支持和协助。”

## 五、安全保障与救济措施

从立法定位来看，《网络安全法》应为网络空间安全的基本法，不可能对协助解密规定得事无巨细。协助解密过程中的安全保障与救济措施可在《网络安全法》的实施细则中予以规定。

### （一）安全保障措施

协助解密不仅涉及当事人的隐私，也可能涉及企业的商业秘密甚至国家秘密。因此，侦查人员和网络服务提供者对协助解密过程中获悉的国家秘密、商业秘密和个人隐私要严格保密，不得泄露、出售或者非法向他人提供，并及时销毁与案件无关的材料。为避免影响案件的调查与侦破，网络服务提供者原则上应对协助解密的行为进行保密，未经执法机关允许在案件侦查期间不得告知用户。

### （二）救济措施

1. 对网络服务提供者的救济

尽管网络服务提供者负有协助解密的法定义务，但是其对于执法机关做出的违法要求，有权向该执法机关或其上级机关提出申诉，以保障企业自身的权益。此外，网络服务提供者在协助解密的过程中产生的费用，有权要求执法机关给予补偿。但是，该费用支出必须是合理的，且与协助解密活动直接相关。

2. 对当事人的救济

对当事人的救济主要是保障当事人的知情权、异议权和损害赔偿请求权。首先，在协助解密行为结束后，执法机关应当将协助解密的有关情况通知当事人，以便于其核对情况是否属实并提出异议、申请排除非法证据等；其次，当事人认为协助解密行为违法或者采用的手段违反必要性原则或比例原则，可以向执法机关依法申请复议；再次，违法实施协助解密给当事人合法权利造成损害的，当事人可以申请国家赔偿。

## 六、结语

网络服务提供者协助解密，始终面临着为了保障国家安全、维护社会公共利益而不得不适用的“现实必要性”和对公民隐私权、企业营业自由构成威胁的“现实危险性”两难选择。在执法机构没有解密能力的情况下，责令网络服务提供者协助解密是成本相对低的途径。为最大限度的减少其产生的外溢效应，立法有必要明确其适用案件种类、适用对象、适用原则以及安全保障措施，赋予当事人知情权、申诉权和申请国家赔偿的权利，从实体和程序两个方面严格限制其适用，使公民对国家行为有“可预测性”，从而保证刑事侦查活动在犯罪控制与人权保障之间实现动态平衡。


参考文献

[1] 马民虎, 果园, 马宁. 自解密义务的法律困惑及其本土适用[J]. 苏州大学学报( 哲学社会科学版), 2016(1): 89–94.
Ma M H, Guo Y, Ma N. Legal issues regarding the self-decryption obligationand its application in China[J]. Journal of Soochow University (Philosophy & Social Science Edition), 2016(1): 89–94.

[2] Jeffrey K. Missing the Metaphor: Compulsory decryption and the fifth amendment[J]. The Boston University Public Interest Law Journal, 2015, 24(53): 54–75.

[3] 谢登科. 论技术侦查中的隐私权保护[J]. 法学论坛, 2016(3): 32–40.
Xie D K. On the protection of privacy rights in technical investigation[J]. Legal Forum, 2016(3): 32–40.

[4] 霍永库, 冯潇洒. 社会角色理论的网络运营者安全保障义务分析[J]. 西安交通大学学报, 2016, 36(1): 62–68.
Huo Y K, Feng X S.The analysis of network operators’ safety guarantee obligation based on the theory of the social role[J]. Journal of Xi’an Jiaotong University, 2016, 36(1): 62–68.

[5] 唐忠民. 公民通信自由和通信秘密保护的两个问题[J]. 法学, 2007(12): 14–17.
Tang Z M. Two issues of the freedom of correspondence and

protection of correspondence secrets [J]. Law Science, 2007 (12):14–17.

[6] 高荣林. 美国电子数据取证之无证搜查与证据排除规则[J]. 上海政法学院学报，2015,30(5): 72–81.
Gao R L. Unlicensed search and evidence exclusion rule of electronic data evidence in the USA [J]. Journal of Shanghai University of Political Science & Law, 2015, 30(5):72–81.

[7] 胡铭. 英法德荷意技术侦查的程序性控制[J]. 环球法律评论, 2013, 35(4): 6–18.
Hu M. Technical detection by procedure regulation in United Kingdom, France, Germany, the Netherlands and Italy[J]. Global Law Review, 2013, 35(4): 6–18.