



合规法律评述
2018年6月

上海
上海市银城中路68号
时代金融中心16楼和19楼
邮编: 200120
电话: +86 21 3135 8666
传真: +86 21 3135 8600

北京
北京市建国门北大街8号
华润大厦4楼
邮编: 100005
电话: +86 10 8519 2266
传真: +86 10 8519 2929

香港
香港中环皇后大道中5号
衡怡大厦27楼
电话: +852 2969 5300
传真: +852 2997 3385

伦敦
1F, 3 More London Riverside
London SE1 2RE
United Kingdom
T: +44 (0)20 3283 4337
D: +44 (0)20 3283 4323

www.llinkslaw.com

SHANGHAI
16F/19F, ONE LUJIAZUI
68 Yin Cheng Road Middle
Shanghai 200120 P.R.China
T: +86 21 3135 8666
F: +86 21 3135 8600

BEIJING
4F, China Resources Building
8 Jianguomenbei Avenue
Beijing 100005 P.R.China
T: +86 10 8519 2266
F: +86 10 8519 2929

HONG KONG
27F, Henley Building
5 Queen's Road Central
Central, Hong Kong
T: +852 2969 5300
F: +852 2997 3385

LONDON
1F, 3 More London Riverside
London SE1 2RE
United Kingdom
T: +44 (0)20 3283 4337
D: +44 (0)20 3283 4323

master@llinkslaw.com

浅析网络运营者刑事责任

On Criminal Liabilities of Network Operators

作者: 潘永建 | 李天航 | 洪馨

This article will briefly analyze the criminal laws that could possibly be violated by network operators, the elements of the crimes, and the criminal consequences.

I. The Crimes that Network Operators may Commit

A. The Crime of Infringing Citizens' Personal Information

According to Article 253 of the Criminal Law and Supreme People's Court ("SPC") and Supreme People's Procuratorate ("SPP")'s Interpretations of Several Issues Concerning the Application of Law in Criminal Cases of Infringement of Citizens' Personal Information ("SPC and SPP Interpretations"), the elements for constituting the crime of infringing citizens' personal information are as follows:

1. Violations of relevant national regulations
2. Certain conducts
3. Criminal threshold

.....
如您需要了解我们的出版物,
请与下列人员联系:

郭建良: (86 21) 3135 8756
Publication@llinkslaw.com

通力律师事务所
www.llinkslaw.com

免责声明: 本出版物仅代表作者本人观点, 不代表通力律师事务所的法律意见或建议。我们明示不对任何依赖本出版物的任何内容而采取或不采取行动所导致的后果承担责任。我们保留所有对本出版物的权利。

浅析网络运营者刑事责任 On Criminal Liabilities of Network Operators

Compliance tips. We remind companies to pay attention to seven typical criminal offences committed by companies in order to avoid criminal investigation.

B. The Crime of Refusing to Fulfill the Obligations of Information Network Security Management

The elements for the crime of refusing to fulfill the obligations of information network security management are as follows:

1. Violations of laws and administrative regulations
2. Certain conducts
3. Causation

Compliance tips. We remind companies to pay attention to five typical criminal offences committed by companies in order to avoid criminal investigation.

II. Suggestions

The best way for companies to avoid the above-mentioned crimes is to build a solid compliance system. We hereby make following recommendations on corporate compliance based on our long-term compliance legal service experience.

1. Collect citizens' personal information in a legal and compliant method.
2. Take the regulatory authority's requirements seriously.
3. Establish and improve internal control systems.

2018年6月1日是中国《网络安全法》正式生效实施一周年之日。为帮助企业清晰理解网安法下企业的责任与义务，通力律师事务所网络安全与数据服务团队从6月1日起陆续推出《<网络安全法>实务30问》系列双语指引，通过对法律规定的解读，结合典型实践案例，深度剖析企业的责任与义务，助力企业合规经营，有效防范风险。

本篇为《<网络安全法>实务30问》系列双语指引的第五篇，简析网络运营者刑事责任的相关问题，以期对相关人士提供参考。

《网络安全法》实施一年以来，网络运营者因违反《网络安全法》等法律法规被行政处罚的案例不在少数。需要提醒企业注意的是，违反《网络安全法》后果并不仅限于行政责任，严重的可能会被判处刑罚。本文将就网络运营者可能触犯的刑事法律、构成要件及后果进行简要分析。

浅析网络运营者刑事责任 On Criminal Liabilities of Network Operators

一. 网络运营者可能触犯哪些罪名

(一) 侵犯公民个人信息罪

1. 构成要件

根据刑法第 253 条之一和《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》(以下简称《两高司法解释》), 判断是否构成侵犯公民个人信息罪的要件有:

(1) 违反国家有关规定

违反国家有关规定是指违反包括法律、行政法规、部门规章在内的国家层面的规定, 与刑法第 96 条规定的“国家规定”相比, 增加了部门规章。因此, 不仅违反《网络安全法》《消费者权益保护法》等法律, 而且违反《电信和互联网用户个人信息保护规定》《网络交易管理办法》等规章有关个人信息保护规定的, 都有可能构成犯罪。

(2) 行为

在前述违反国家有关规定的前提下, 下列行为可能构成犯罪:

- a) 出售公民个人信息的;
- b) 向特定人提供公民个人信息, 以及通过信息网络或者其他途径发布公民个人信息的;
- c) 未经被收集者同意, 将合法收集的公民个人信息向他人提供的, 但经过处理无法识别特定个人且不能复原的除外;
- d) 窃取公民个人信息的;
- e) 通过购买、收受、交换等方式获取公民个人信息;
- f) 在履行职责、提供服务过程中收集公民个人信息的。

(3) 入刑标准

实施前述第 2 项所列行为, 达到以下条件的, 将被追究刑事责任:

种类	数量标准		特殊标准	为合法经营活动而非非法购买、收受
	基础数量	不同种类折算		

浅析网络运营者刑事责任

On Criminal Liabilities of Network Operators

行踪轨迹	50 条	按照一 定比例 折算达 基础标 准	被他人 用于犯 罪	知道或 者应当 知道将 公民个 人信息 用于犯 罪	不适用											
通信内容	50 条		不适用													
征信信息																
财产信息																
其他可能 影响人 身、财产 安全的	住宿信息							500 条								
	通信记录															
	健康生理 信息															
	交易信息															
其他																
其他公民个人信息	5000 条													获利 5 万元		
违法所得	5000 元															
在履行职责或者提供服务过程中获得的公民个人信息	上述数量的一半															
曾有侵犯公民个人信息 行为	之前(无时间限制)有一次被刑事处罚															
	之前二年内有一次被行政处罚															
其他严重情形																

2. 合规提示

基于上述分析，结合本所的执业经验，我们提醒企业应注意以下场景，避免因涉嫌刑事犯罪被调查：

- a) 企业向第三方出售公民个人信息或者出售的数据中含有公民个人信息的；
- b) 企业让第三方以该第三方名义采取调查问卷等形式获取公民个人信息后再转给企业，并由企业支付一定费用的；
- c) 企业从第三方处购买的数据中含有公民个人信息，或者直接购买公民个人信息的；
- d) 企业接受第三方提供的公民个人信息，未获得个人信息主体同意或者授权，或者存在其他违反国家有关规定的情形的；
- e) 企业转让个人信息，或者与第三方交换、共享个人信息，但未获得该个人信息主体的合法授权或者同意的；
- f) 企业在经营中收集公民个人信息过程中，未通过隐私政策、与个人信息主体签署协议等形式获得个人信息主体的授权或者同意；
- g) 开展征信业务的企业向没有获得征信主体合法授权的企业或者个人提供征信主体的

浅析网络运营者刑事责任 On Criminal Liabilities of Network Operators

征信信息的。

(二) 拒不履行信息网络安全管理义务罪

1. 构成要件

根据刑法第二百八十六条之一和《两高司法解释》，判断是否构成拒不履行信息网络安全管理义务罪的要件有：

(1) 违反法律、行政法规规定

与侵犯公民个人信息罪不同的是，构成该罪的前提必须为违反法律、行政法规规定的信息网络安全管理义务，如《网络安全法》《计算机信息系统安全保护条例》等，违反部门规章不能构成该罪。

(2) 行为

违反法律、行政法规规定的信息网络安全管理义务要求，经监管部门责令采取改正措施而拒不改正的行为可能构成犯罪。

a) 责令采取改正措施

- i. 一般情况下，责令改正须为书面作出；
- ii. 对于监管部门口头要求违法的企业改正的，在司法实践中由于难以证明监管部门作出责令改正的要求而难以认定。但是如果监管部门通过对企业负责人或者直接负责的主管人员通过做笔录形式责令改正，且该负责人或者直接负责的主管人员签字确认的，也符合该罪关于责令改正的要求；
- iii. 对于企业违法的行为如果作出行政处罚的，也应当视为已经做出责令改正的要求，因为改正违法行为是行政处罚的内在要求，被处罚的行为应当予以改正；
- iv. 责令改正应有明确的要求，如责令日志留存必须达到 6 个月的要求等，模糊或者笼统的要求使企业难以执行。

b) 拒不改正

- i. 对监管部门的决定采取不作为形式的，当然视为拒不改正；
- ii. 正在采取改进措施或者正在准备采取改进措施但尚未完全改正的，可以作为抗辩的理由，尤其是对于以下情况，被采纳的可能性较大：
 - i) 因客观原因导致改正措施尚未完成的，如硬件已经采购但企业尚未收到等；
 - ii) 改正措施需要较长时间和较大工作量，接到监管部门责令改正决定即开始着手实施的；

浅析网络运营者刑事责任 On Criminal Liabilities of Network Operators

- iii) 已经聘请专门机构或者供应商实施改正措施，但因该专门机构或者供应商原因导致未完成改正工作。

(3) 入刑标准

上述行为构成拒不履行信息网络安全管理义务罪还须以行为造成以下后果为前提：

- a) 致使违法信息大量传播的；
- b) 致使用户信息泄露，造成严重后果的；
- c) 致使刑事案件证据灭失，情节严重的；
- d) 有其他严重情节的。

2. 合规提示

基于上述分析，结合本所的执业经验，我们提醒企业应注意以下场景，避免因涉嫌刑事犯罪而被调查：

- a) 企业未依法开展网络安全等级保护定级并履行等级保护义务，被公安机关责令改正后，既未委托等保评测机构进行评测定级，也没有对照法律要求采取安全保护措施，致使企业存储的大量个人信息泄露，或者发生刑事案件后，致使证据灭失的；
- b) 企业未履行网络实名制义务，对用户核实真实身份信息，经监管部门责令改正拒不改正，在该用户实施刑事犯罪后，无法查证犯罪嫌疑人的；
- c) 企业未制定网络安全应急预案，经监管部门责令改正后拒不改正发生黑客攻击等网络安全事件，导致企业存储的大量个人信息泄露的；
- d) 企业未采取技术措施和其他必要措施，确保其收集的个人信息安全，被监管部门责令改正拒不改正，导致个人信息大量泄露的；
- e) 互联网信息服务提供者对其用户发布的信息未尽到加强管理义务，未采取对违法违规信息的停止传输、消除等处置措施，保存有关记录，经监管部门责令改正拒不改正，导致违法信息大量传播或者证据无法固定的。

二. 建议

企业做好合规工作是避免触犯侵犯公民个人信息罪和拒不履行信息网络安全管理义务罪最好的途径。我们根据长期的合规法律服务经验提出以下建议，供企业参考。

1. 合法、合规收集公民个人信息。梳理本企业收集、使用、转让、共享、交换等处置公民个人信息的环节，对照法律、行政法规和部门规章的要求，开展合规审查和改正工作。
2. 重视监管部门的管理。正确履行信息网络安全管理义务，尤其是对于监管部门检查后作出的处罚决定、责令改正决定等，应当积极采取改正措施。即使不具备条件或者无法立即改正的，也应当做好准备工作，制定工作计划。
3. 建立健全内控制度。加强企业内控制度建设，做好员工的教育管理工作，避免因员工个人的犯罪行为致使企业遭受查处或者处罚。

浅析网络运营者刑事责任

On Criminal Liabilities of Network Operators

<p>《<网络安全法>实务 30 问》系列双语指引问题清单 Schedule of “30 Questions About CSL”</p>	
1	《网络安全法》体系下企业的责任与义务概览 Summary of Companies’ Responsibilities and Liabilities under the CSL
2	企业如何落实网络安全等级保护义务 How Should Companies Implement the Graded Network Security Protection System
3	企业正确应对国家机关调取数据的实务分析 How Should Companies Properly Respond to Authorities’ Requirement for Data Access?
4	企业使用微信企业号的合规要点 Key Compliance Issues in Using Enterprise WeChat
5	浅析网络运营者的刑事责任 Criminal Liabilities of Network Operators
6	VPN 使用与跨境联网的合规要点 Key Compliance Issues in Use of VPN and Cross-border Connectivity
7	互联网信息服务提供者责任义务辨析 Analysis on The Responsibilities and Obligations of Internet Information Services Providers
8	隐私政策的合规要点与最佳实践 Key Compliance Issues and Best Practices for Privacy Policies
9	企业与第三方关于个人信息保护责任划分 Division of Responsibilities Between Companies and Third Parties Regarding Personal Information Protection
10	员工信息收集、使用合规要点 Key Compliance Issues in Collection and Use of Employee Information
11	数据出境比你想象的常见——数据出境情形分析 Data Cross-border Transfer Happens More Than You Imagine – Analysis of Data Cross-border Transfer Scenarios
12	个人信息安全事件的妥善应对 Proper Response to Personal Information Security Incidents
13	个人信息和重要数据本地化存储的实务分析 Practical Analysis on Local Storage of Personal Information and Important Data
14	网络安全事件应对-兼论网络安全应急预案的必要性 Network Security Emergency Response and Discussion on Necessity of Network Security Emergency Plans
15	网络关键设备、网络安全专用产品、网络产品及服务涉及的网络安全审查制度 Network Security Review on Key Network Equipment, Specialized Network Products and Network Products and Services

免责声明：本出版物仅代表作者本人观点，不代表通力律师事务所的法律意见或建议。我们明示不对任何依赖本出版物的任何内容而采取或不采取行动所导致的后果承担责任。我们保留所有对本出版物的权利。

浅析网络运营者刑事责任

On Criminal Liabilities of Network Operators

16	网络安全负责人的设立及职责辨析 Analysis on Network Security Officer and Its Duties and Responsibilities
17	个人信息使用合规分析 Compliance Analysis on Use of Personal Information
18	企业与员工关于个人信息保护的责任划分 Division of Responsibilities Between Companies and Employees Regarding Personal Information Protection
19	企业应当如何落实网络信息实名制要求 How Should Companies Implement Network Information Real-Name Requirements
20	中国法下的个人信息概念与范围辨析 Analysis on Definition and Scope of Personal Information Under PRC Law
21	客户信息收集、使用合规要点 Key Compliance Issues in Collection and Use of Customer Information
22	电商等行业使用个人信息的合规要点 Key Compliance Issues for Use of Personal Information in E-Commerce [etc.]
23	《信息安全技术 个人信息安全规范》作为推荐性国家标准（GB/T）的实践价值分析 Practical Value Analysis on <i>Information Security Technology – Personal Information Security Specification</i> as a Recommended National Standard (GB/T)
24	收购兼并中涉及数据尽职调查要点分析 Key Issues of Data Due Diligence in M&A
25	浅析企业的个人信息保护义务 Brief Analysis on Companies' Obligations of Personal Information Protection
26	关键信息基础设施的界定 Definition of Key Information Infrastructures
27	关键信息基础设施运营者的责任与义务 The Responsibilities and Obligations of Key Information Infrastructure Operators
28	重要数据的界定 Identification of Important Data
29	如何进行数据出境？——数据出境的基本流程 How to Transfer Data Abroad? – The Basic Process of Data Cross-border Transfer.
30	数据出境评估 Assessment for Data Cross-border Transfer

浅析网络运营者刑事责任 On Criminal Liabilities of Network Operators

如需进一步信息，请联系：

作者	
潘永建 电话: +86 21 3135 8701 david.pan@linkslaw.com	
上海	
俞卫锋 电话: +86 21 3135 8686 david.yu@linkslaw.com	刘贇春 电话: +86 21 3135 8678 bernie.liu@linkslaw.com
余 铭 电话: +86 21 3135 8770 selenashe@linkslaw.com	娄斐弘 电话: +86 21 3135 8783 nicholas.lou@linkslaw.com
钱大立 电话: +86 21 3135 8676 dali.qian@linkslaw.com	孔焕志 电话: +86 21 3135 8777 kenneth.kong@linkslaw.com
吴 炜 电话: +86 21 6043 3711 david.wu@linkslaw.com	潘永建 电话: +86 21 3135 8701 david.pan@linkslaw.com
姜 琳 电话: +86 21 6043 3710 elyn.jiang@linkslaw.com	
北京	
俞卫锋 电话: +86 10 8519 2266 david.yu@linkslaw.com	刘贇春 电话: +86 10 8519 2266 bernie.liu@linkslaw.com
杨玉华 电话: +86 10 8519 1606 yuhua.yang@linkslaw.com	
香港(与张慧雯律师事务所有限法律责任合伙联营)	
俞卫锋 电话: +86 21 3135 8686 david.yu@linkslaw.com	吕 红 电话: +86 21 3135 8776 sandra.lu@linkslaw.com
伦敦	
杨玉华 电话: +44 (0)20 3283 4337 yuhua.yang@linkslaw.com	

© 《<网络安全法>实务 30 问》系列双语指引独家授权威科先行网络安全与数据合规模块在线发布

免责声明：本出版物仅代表作者本人观点，不代表通力律师事务所的法律意见或建议。我们明示不对任何依赖本出版物的任何内容而采取或不采取行动所导致的后果承担责任。我们保留所有对本出版物的权利。