

# 国家/地区聚焦报告： 中国互联网相关政策 倡议和法律

温尼·马科夫斯基 (Veni Markovski) 和  
阿列克谢·特雷皮卡林 (Alexey Trepykhalin)  
2022 年 1 月 31 日  
GE-010 (最新动态)



---

## 目录

简介	3
中国的外交政策声明和倡议	3
国内声明、立法和法规	6
结语	9
附录 1	10
中华人民共和国网络安全法	10
附录 2	19
中国工业和信息化部互联网域名管理办法（节选）	19
附录 3	21
中国互联网域名体系（节选）	21
附录 4	22
中华人民共和国数据安全法（节选）	22
附录 5	24
中华人民共和国个人信息保护法	24
附录 6	33
关键信息基础设施安全保护条例（节选）	33

---

## 简介

本文件介绍中国在 2015 年 12 月 16 日至 2021 年 11 月 5 日期间提出的互联网相关政策倡议和法律/法规；旨在确保 ICANN 社群获得必要信息，以加深其对联合国、国际电信联盟 (ITU) 和其他联合国机构正在进行的审议工作的了解。

本文是定期发布的国别报告系列的一部分，这些报告旨在概述与互联网生态系统和 ICANN 使命有关的活动。对此类活动的监控是 ICANN 组织的政府和国际政府间组织合作 (GE) 团队的一项基本职责，即，让更广泛的 ICANN 社群了解全球单一且可互操作的互联网及其唯一标识符系统的重要问题。<sup>1</sup>

与先前的 GE 文件一样，这份报告基于与互联网政策和技术相关的主要源内容，这些内容涉及域名系统 (DNS)、互联网协议 (IP) 地址和协议参数等。此外，本文件依赖于有关中国在联合国 (U.N.)、国际电信联盟 (ITU) 以及国内就这些相同问题所持立场的相关内容、声明和法律/法规条款。

## 中国的外交政策声明和倡议

2015 年 12 月 16 日，中华人民共和国主席习近平在乌镇<sup>2</sup>举行的第二届世界互联网大会开幕式上发表讲话，表示：“...国际社会应该在相互尊重、相互信任的基础上，加强对话合作，推动互联网全球治理体系变革，共同构建和平、安全、开放、合作的网络空间，建立多边、民主、透明的全球互联网治理体系。”<sup>3</sup>

为实现此目的，习主席表示，需要将“尊重各个国家/地区网络主权”、“平等参与国际网络空间治理”作为四项指导原则之一。<sup>4</sup>习主席还补充到，“国际网络空间治理，应该坚持多边参与、多方参与，由大家商量着办，发挥政府、国际组织、互联网企业、技术社群、民间机构、公民个人等各个主体作用，不搞单边主义，不搞一方主导或由几方凑在一起说了算。各国应该加强沟通交流，完善网络空间对话协商机制，研究制定全球互联网治理规则，使全球互联网治理体系更加公正合理，更加平衡地反映大多数国家意愿和利益。”<sup>5</sup>

2015 年 3 月 7 日，在 ICANN 政府咨询委员会 (GAC) 会议上，中国代表强调，习主席在 2015 年乌镇第二届世界互联网大会上提出的“四项原则和五点主张”“为我们提供了 [音频不清晰]，同时考虑了中国对互联网治理的思考和立场。”<sup>6</sup>

---

<sup>1</sup> “ICANN 运营和财务规划”，第 47 页，ICANN 组织，2020 年 12 月，<https://www.icann.org/en/system/files/files/draft-op-financial-plan-fy21-25-opplan-fy21-20dec19-en.pdf>。

<sup>2</sup> 世界互联网大会由中国国家互联网信息办公室和浙江省人民政府在浙江省乌镇举行，每年举办一次：<https://www.wicwuzhen.cn/>，英文翻译链接：[http://www.wuzhenwic.org/2020-10/15/c\\_547699.htm](http://www.wuzhenwic.org/2020-10/15/c_547699.htm)。

<sup>3</sup> 中华人民共和国主席习近平在第二届世界互联网大会开幕式上的讲话，乌镇，2015 年 12 月 16 日：[https://www.mfa.gov.cn/web/zyxw/201512/t20151216\\_336173.shtml](https://www.mfa.gov.cn/web/zyxw/201512/t20151216_336173.shtml)，英文翻译链接：[https://www.fmprc.gov.cn/eng/wjdt\\_665385/zyjh\\_665391/201512/t20151224\\_678467.html](https://www.fmprc.gov.cn/eng/wjdt_665385/zyjh_665391/201512/t20151224_678467.html)。

<sup>4</sup> 中华人民共和国主席习近平的讲话。

<sup>5</sup> 中华人民共和国主席习近平的讲话。

<sup>6</sup> 马拉喀什 - GAC 高层政府级会议，2016 年 3 月 7 日（星期一），ICANN55 | 摩洛哥，马拉喀什，第 86 页 <https://gac.icann.org/transcripts/public/transcript-icann55-gac-hl-governmental-meeting-2016-03-07.pdf>。

2016年4月27日，中国发布了《国家网络空间安全战略》，<sup>7</sup>阐明了各国在“加强网络空间国际合作”方面的重要性。为此，该战略详细说明了这种合作应当“推进全球互联网治理体系变革”以及“推动互联网地址、根域名服务器等基础资源管理国际化”。该战略还表示，支持“联合国发挥主导作用，推动制定各方普遍接受的网络空间国际规则、网络空间国际反恐公约，健全打击网络犯罪司法协助机制，深化在政策法律、技术创新、标准规范、应急响应、关键信息基础设施保护等领域的国际合作”，它还呼吁“建立多边、民主、透明的国际互联网治理体系”。

2017年3月2日，中国发布了《网络空间国际合作战略》。<sup>8</sup>该战略指出，“中国将推进联合国互联网治理论坛机制改革，促进论坛在互联网治理中发挥更大作用。加强论坛在互联网治理事务上的决策能力，推动论坛获得稳定的经费来源，在遴选相关成员、提交报告等方面制定公开透明的程序。”《网络空间国际合作战略》还指出，中国将“参加旨在促进互联网关键资源公平分配和管理的国际讨论”，并且其将“积极推动互联网名称和数字地址分配机构国际化改革，使其成为具有真正独立性的国际机构，不断提高其代表性和决策、运行的公开透明。”<sup>9</sup>

2018年4月20日，在北京召开的全国网络安全和信息化工作会议上，习主席表示，“今后，推进全球互联网治理体系变革是大势所趋、人心所向。”他还补充表示，“国际网络空间治理应该坚持多边参与、多方参与，发挥政府、国际组织、互联网企业、技术社群、民间机构、公民个人等各种主体作用。既要推动联合国框架内的网络治理，也要更好发挥各类非国家行为体的积极作用。”<sup>10</sup>

2019年7月9日，中国在其向国际安全背景下信息和电信领域的发展不限成员名额工作组(OEWG)提交的材料中指出：“各国应当共同协作，建立多边、民主和透明的全球互联网治理体系。负责根服务器等关键资源管理的组织应真正不受任何国家的控制，确保所有国家的广泛参与以及共同决策。”<sup>11</sup>

2020年4月，中国针对联合国 OEWG 前期报告草案提交了以下内容贡献提案，其中指出：“鉴于我们的时间有限，因此还应注意避免在报告中引入尚未获得全球共识的概念（例如‘公共核心’），”并且：“在前两届会议上，包括中国在内的各方就网络主权、供应链安全、保护关键

<sup>7</sup> 中国版权和传媒，《国家网络空间安全战略》，于2016年12月27日更新：

[http://www.cac.gov.cn/2016-12/27/c\\_1120195926.htm](http://www.cac.gov.cn/2016-12/27/c_1120195926.htm)，非官方英文翻译链接：

<https://chinacopyrightandmedia.wordpress.com/2016/12/27/national-cyberspace-security-strategy/>。

<sup>8</sup> 《网络空间国际合作战略》，中国日报，2017年3月2日：[http://www.china.org.cn/chinese/2017-03/07/content\\_40424606.htm](http://www.china.org.cn/chinese/2017-03/07/content_40424606.htm)，非官方英文翻译链接：[https://www.chinadaily.com.cn/kindle/2017-03/02/content\\_28409210.htm](https://www.chinadaily.com.cn/kindle/2017-03/02/content_28409210.htm)。

<sup>9</sup> 《网络空间国际合作战略》，中国日报，2017年3月2日。

<sup>10</sup> 习近平 4月20日在全国网络安全和信息化工作会议上的讲话，2018年4月30日：[http://www.xinhuanet.com/politics/2018-04/21/c\\_1122719810.htm](http://www.xinhuanet.com/politics/2018-04/21/c_1122719810.htm)，非官方英文翻译链接：

<https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-xi-jinpings-april-20-speech-national-cybersecurity-and-informatization-work-conference/>。

<sup>11</sup> 中国向国际安全背景下信息和电信领域的发展不限成员名额工作组提交的材料，2019年7月7日。

<https://s3.amazonaws.com/unoda-web/wp-content/uploads/2019/09/china-submissions-oewg-en.pdf>。

---

基础设施、避免单方面制裁和打击网络恐怖主义等问题提出了数十项建设性提案。希望这些提案能够纳入到报告中。”<sup>12</sup>

2020年9月8日，中国外交部发布了一份《全球数据安全倡议》，其中强调了各国在数据安全、网络犯罪等领域加强合作的必要性。该文件建议“政府、国际组织、ICT<sup>13</sup>企业、技术社群、民间机构和公民个人等各主体秉持共商共建共享理念，齐心协力促进数据安全”。该文件还呼吁各国“以事实为依据全面客观看待数据安全问题，积极维护全球 ICT 产品和服务的供应链开放、安全、稳定”。<sup>14</sup>

2021年3月，年度“两会”立法大会通过了“十四五规划”和2035年远景目标，其中第十八章（“营造良好数字生态”）第四节（“推动构建网络空间命运共同体”）指出：“推进网络空间国际交流与合作，推动以联合国为主渠道、以联合国宪章为基本原则制定数字和网络空间国际规则。推动建立多边、民主、透明的全球互联网治理体系，建立更加公平合理的网络基础设施和资源治理机制。”<sup>15</sup>

2021年3月10日，在联合国 OEWG 审议期间，中国指出：“各国应平等参与国际互联网资源的管理和分配。”<sup>16</sup>

2021年6月29日，中国和俄罗斯联邦发表了一项联合声明，同意将现有的双边《中俄睦邻友好合作条约》延期。在联合声明中，双方同意“重申将巩固国际信息安全领域的双、多边合作”，并强调，“双方在国际互联网治理，包括保障各国平等参与治理、增强各国在该进程中的作用、国家保有国内互联网治理主权等问题上持相同立场。俄罗斯和中国强调需要加强国际电信联盟作用，以及该组织领导机构中应有两国派遣的代表。”<sup>17</sup>

---

<sup>12</sup> 中国针对 OEWG 前期报告草案初稿提交的内容贡献提案，2020年4月16日（PDF 属性中标注的日期），<https://front.un-arm.org/wp-content/uploads/2020/04/china-contribution-to-oewg-pre-draft-report-final.pdf>。

<sup>13</sup> ICT - 信息和通信技术，UNTERM - 联合国术语数据库，<https://unterm.un.org/unterm/display/record/imo/na?OriginalId=551772be82184a22adaeb86841e335e6>。

<sup>14</sup> 《全球数据安全倡议》，中国外交部网站，2020年9月8日：<https://www.fmprc.gov.cn/chn/pds/ziliao/tytj/t1827469.htm>，英文翻译链接：[https://www.fmprc.gov.cn/mfa\\_eng/wjb\\_663304/zzjg\\_663340/jks\\_665232/kjfywj\\_665252/202009/t20200908\\_599773.html](https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjfywj_665252/202009/t20200908_599773.html)，以及“中国发起一项反对将数据安全问题政治化的全球数据安全倡议”，路透社，2020年9月7日，<https://www.reuters.com/article/wangyi-global-digital-security-0908-idCNKBS25Z0AJ>。

<sup>15</sup> 观察者，“十四五”规划和2035年远景目标纲要（全文），2021年3月13日，[https://www.guancha.cn/politics/2021\\_03\\_13\\_583945\\_5.shtml](https://www.guancha.cn/politics/2021_03_13_583945_5.shtml)。

<sup>16</sup> 国际安全背景下信息和电信领域的发展不限成员名额工作组，第三次实质性会议，2021年3月8日至12日，OEWG 主席总结，会议室文件，2021年3月10日，A/AC.290/2021/CRP.3\*，<https://front.un-arm.org/wp-content/uploads/2021/03/Chairs-Summary-A-AC.290-2021-CRP.3-technical-reissue.pdf>。

<sup>17</sup> 俄罗斯联邦驻大不列颠及北爱尔兰联合王国大使馆，中华人民共和国和俄罗斯联邦关于《中俄睦邻友好合作条约》签署20周年的联合声明，2021年6月28日：[http://www.xinhuanet.com/2021-06/28/c\\_1127606620.htm](http://www.xinhuanet.com/2021-06/28/c_1127606620.htm)[http://www.xinhuanet.com/2021-06/28/c\\_1127606620.htm](http://www.xinhuanet.com/2021-06/28/c_1127606620.htm)，非官方英文翻译链接：<https://www.rusemb.org.uk/fnapr/7007>。

---

2021 年 11 月 1 日，俄罗斯联邦递交了拟议的《联合国打击网络犯罪公约》草案文本<sup>18</sup>，并宣布该文本由中国共同提出。<sup>19-20</sup>

2021 年 11 月 5 日，中国在联合国特设委员会 (AHC) 的第一次会议上提出提案。<sup>21</sup>其中指出：“要求各成员国应将侵入、破坏信息和通信技术设施、系统、数据或关键信息基础设施的行为规定为犯罪。可包括：非法访问计算机信息系统、非法干扰计算机信息系统、非法获取计算机数据、非法干扰计算机数据、侵犯关键信息基础设施等。”

## 国内声明、立法和法规

2015 年 7 月 1 日，《国家安全法》通过。其中指出（第五十九条）：“国家建立国家安全审查和监管的制度和机制，对影响或者可能影响国家安全的外商投资、特定物项和关键技术、网络信息技术产品和服务、涉及国家安全事项的建设项目，以及其他重大事项和活动，进行国家安全审查，有效预防和化解国家安全风险。”<sup>22</sup>该法律第二十五条规定：“国家建设网络与信息安全保障体系，[...] 加强网络管理，维护国家网络空间主权、安全和发展利益。”

《网络安全法》(CSL) 自 2017 年 6 月 1 日起施行。该法律规定，国家有责任“推动构建和平、安全、开放、合作的网络空间，建立多边、民主、透明的网络治理体系”。该法律还规定应当在“中国大陆”存储国内的互联网数据。该法律第三十一条界定了关键信息基础设施的范围以“对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务以及其他关键信息基础设施建立多层次的网络安全保护体系”。该法律第三十七条规定，“因业务需要，确需向境外提供的[个人信息、重要数据]，[关键信息基础设施的运营者]应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定。”<sup>23</sup>（相关条款见本文件的附录 1。）

2017 年 8 月 24 日，中国工业和信息化部 (MIIT) 发布了修订的《互联网域名管理办法》。<sup>24</sup>（相关条款见本文件的附录 2。）

---

<sup>18</sup> 关于打击出于犯罪目的使用信息和通信技术的行为的联合国公约，2021 年 7 月 27 日，[https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Comments/RF\\_28\\_July\\_2021\\_-\\_E.pdf](https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Comments/RF_28_July_2021_-_E.pdf)。

<sup>19</sup> 关于打击网络犯罪的新联合国公约即将施行，fm4.orf.at，<https://fm4.orf.at/stories/3019118/>。

<sup>20</sup> 康斯坦丁·科迈蒂斯 (Konstantinos Komaitis)，Twitter 帐户，2021 年 11 月 1 日和 2022 年 1 月 19 日，<https://twitter.com/i/web/status/1455217317504327683>。

<sup>21</sup> 中国对联合国打击为犯罪目的使用信息和通信技术公约范围、目标和框架（要素）的建议：[https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First\\_session/Comments/Chinas\\_Suggestions\\_on\\_the\\_Scope\\_Objectives\\_and\\_Structure\\_AHC\\_ENG.pdf](https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/Comments/Chinas_Suggestions_on_the_Scope_Objectives_and_Structure_AHC_ENG.pdf)。

<sup>22</sup> 《中华人民共和国国家安全法》，2015 年 7 月 1 日：[http://www.gov.cn/zhengce/2015-07/01/content\\_2893902.htm](http://www.gov.cn/zhengce/2015-07/01/content_2893902.htm)，非官方英文翻译链接：<https://www.chinalawtranslate.com/en/2015nsl/>。

<sup>23</sup> 《中华人民共和国网络安全法》（自 2017 年 6 月 1 日起施行）：[http://www.cac.gov.cn/2016-11/07/c\\_1119867116.htm](http://www.cac.gov.cn/2016-11/07/c_1119867116.htm)，非官方英文翻译链接：<https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/>。

<sup>24</sup> 工业和信息化部，《互联网域名管理办法》，2017 年 8 月 24 日：[http://www.cac.gov.cn/2017-09/28/c\\_1121737753.htm](http://www.cac.gov.cn/2017-09/28/c_1121737753.htm)，非官方英文翻译链接：<https://www.chinalawtranslate.com/en/internet-domain-name-management-measures/>。

---

2018 年 1 月 29 日，在上述的新办法第五条的基础上，MIIT 宣布了调整后的中国互联网域名体系。<sup>25</sup>（相关条款见本文件的附录 3。）

---

<sup>25</sup> 从 2021 年 8 月 19 日开始，中文来源的 URL 失效，英文来源的链接为：  
<https://www.chinalawtranslate.com/en/chinese-internet-domain-name-system/>。

2019年6月13日,《个人信息出境安全评估办法》第二条提出:“网络运营者向境外提供在中华人民共和国境内运营中收集的个人信息(以下称个人信息出境),应当按照本办法进行安全评估。经安全评估认定个人信息出境可能影响国家安全、损害公共利益,或者难以有效保障个人信息安全的,不得出境。国家关于个人信息出境另有规定的,从其规定。”<sup>26</sup>

2021年6月10日,第十三届全国人民代表大会常务委员会第二十九次会议通过了《数据安全法》(DSL)。<sup>27</sup>(参见本文件附录4中的相关法律文本。)

2021年7月30日,新的《关键信息基础设施安全保护条例》发布(中国国务院2021年4月27日通过后)。该条例界定了关键信息基础设施的范围,针对“行业和领域”制定了相关条款以进一步详细说明其范围,并且规定了在发生“特别重大网络安全事件”(例如“较大规模”个人信息泄露)时,这些机构向中央网络权威机构进行报告的要求。<sup>28</sup>该条例自2021年9月1日起施行。(该条例的相关条款见本文件的附录6。)

2021年8月20日,中华人民共和国全国人民代表大会常务委员会通过了《个人信息保护法》(PIPL)。该法律自2021年11月1日起施行。“为了保护个人信息权益,规范个人信息处理活动,促进个人信息合理利用[...]制定本法。”“自然人的个人信息受法律保护,任何组织、个人不得侵害自然人的个人信息权益。”“在中华人民共和国境内处理自然人个人信息的活动,适用本法。”“在中华人民共和国境外处理中华人民共和国境内自然人个人信息的活动,有下列情形之一的,也适用本法:”(一)“以向境内自然人提供产品或者服务为目的;”(二)“分析、评估境内自然人的行为;”(三)“法律、行政法规规定的其他情形。”该法律还定义了个人信息及其处理中包含的内容:“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。个人信息的处理包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等。”<sup>29</sup>(该法律全文见本文件的附录5。)

<sup>26</sup> 关于个人信息出境的新规定草案“个人信息出境安全评估办法(征求意见稿)”,2019年6月13日:[http://www.cac.gov.cn/2019-06/13/c\\_1124613618.htm](http://www.cac.gov.cn/2019-06/13/c_1124613618.htm),非官方英文翻译链接:<https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-new-draft-rules-cross-border-transfer-personal-information-out-china/>。

<sup>27</sup> Inside Privacy,非官方翻译,科文顿·柏灵律师事务所敬上:“个人信息出境安全评估办法(征求意见稿)”,2019年6月13日:[https://www.insideprivacy.com/wp-content/uploads/sites/51/2019/06/Measures-for-Security-Assessment-of-the-Cross-Border-Transfer-of-Personal-Information\\_bilingual.pdf](https://www.insideprivacy.com/wp-content/uploads/sites/51/2019/06/Measures-for-Security-Assessment-of-the-Cross-Border-Transfer-of-Personal-Information_bilingual.pdf);以及关于个人信息出境的新规定草案“个人信息出境安全评估办法(征求意见稿)”,2019年6月13日:[http://www.cac.gov.cn/2019-06/13/c\\_1124613618.htm](http://www.cac.gov.cn/2019-06/13/c_1124613618.htm),非官方英文翻译链接:<https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-new-draft-rules-cross-border-transfer-personal-information-out-china/>。

<sup>28</sup> 中华人民共和国国务院令 第745号,2021年7月30日:[http://www.gov.cn/jzhqce/content/2021-08/17/content\\_5631671.htm?trs=1](http://www.gov.cn/jzhqce/content/2021-08/17/content_5631671.htm?trs=1),非官方英文翻译链接:<https://digichina.stanford.edu/news/translation-critical-information-infrastructure-security-protection-regulations-effective-sept>。

<sup>29</sup> 《中华人民共和国个人信息保护法》,(2021年8月20日第十三届全国人民代表大会常务委员会第三十次会议通过),<http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml>。



---

## 结语

中国一直在积极参与联合国所有与网络相关的讨论。中国在国际和国内的内容贡献提案有可能触及 ICANN 的使命。当此类声明或提案涉及到技术互联网治理或 ICANN 使命时，ICANN 组织将通过其政府合作团队继续向 ICANN 社群提供相关信息。

---

## 附录 1

### 中华人民共和国网络安全法<sup>30</sup>

于 2016 年 11 月 6 日通过。自 2017 年 6 月 1 日起施行。

#### 1. 目录

第一章：总则

第二章：网络安全支持与促进

第三章：网络运行安全

第一节：一般规定

第二节：关键信息基础设施的运行安全

第四章：网络信息安全

第五章：监测预警与应急处置

第六章：法律责任

第七章：附则

#### 第一章：总则

**第一条：**为了保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展，制定本法。

**第二条：**在中华人民共和国境内建设、运营、维护和使用网络，以及网络安全的监督管理，适用本法。

**第三条：**国家坚持网络安全与信息化发展并重，遵循积极利用、科学发展、依法管理、确保安全的方针，推进网络基础设施建设和互联互通，鼓励网络技术创新和应用，支持培养网络安全人才，建立健全网络安全保障体系，提高网络安全保护能力。

**第四条：**国家制定并不断完善网络安全战略，明确保障网络安全的基本要求和主要目标，提出重点领域的网络安全政策、工作任务和措施。

**第五条：**国家采取措施，监测、防御、处置来源于中华人民共和国境内外的网络安全风险和威胁，保护关键信息基础设施免受攻击、侵入、干扰和破坏，依法惩治网络违法犯罪活动，维护网络空间安全和秩序。

**第六条：**国家倡导诚实守信、健康文明的网络行为，推动传播社会主义核心价值观，采取措施提高全社会的网络安全意识和水平，形成全社会共同参与促进网络安全的良好环境。

**第七条：**国家积极开展网络空间治理、网络技术研发和标准制定、打击网络违法犯罪等方面的国际交流与合作，推动构建和平、安全、开放、合作的网络空间，建立多边、民主、透明的网络治理体系。

---

<sup>30</sup> 《中华人民共和国网络安全法》（自 2017 年 6 月 1 日起施行）：[http://www.cac.gov.cn/2016-11/07/c\\_1119867116.htm](http://www.cac.gov.cn/2016-11/07/c_1119867116.htm)，非官方英文翻译链接：

<https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/>。

---

**第八条：**国家网信部门负责统筹协调网络安全工作和相关监督管理工作。国务院电信主管部门、公安部门和其他有关机关依照本法和有关法律、行政法规的规定，在各自职责范围内负责网络安全保护和监督管理工作。

县级以上地方人民政府有关部门的网络安全保护和监督管理职责，按照国家有关规定确定。

**第九条：**网络运营者开展经营和服务活动，必须遵守法律、行政法规，尊重社会公德，遵守商业道德，诚实信用，履行网络安全保护义务，接受政府和社会的监督，承担社会责任。

**第十条：**建设、运营网络或者通过网络提供服务，应当依照法律、行政法规的规定和国家标准的强制性要求，采取技术措施和其他必要措施，保障网络安全、稳定运行，有效应对网络安全事件，防范网络违法犯罪活动，维护网络数据的完整性、保密性和可用性。

**第十一条：**网络相关行业组织按照章程，

加强行业自律，制定网络安全行为规范，指导会员加强网络安全保护，提高网络安全保护水平，促进行业健康发展。

**第十二条：**国家保护公民、法人和其他组织依法使用网络的权利，促进网络接入普及，提升网络服务水平，为社会提供安全、便利的网络服务，保障网络信息依法有序自由流动。

任何个人和组织使用网络应当遵守宪法法律，遵守公共秩序，尊重社会公德，不得危害网络安全，不得利用网络从事危害国家安全、荣誉和利益，煽动颠覆国家政权、推翻社会主义制度，煽动分裂国家、破坏国家统一，宣扬恐怖主义、极端主义，宣扬民族仇恨、民族歧视，传播暴力、淫秽色情信息，编造、传播虚假信息扰乱经济秩序和社会秩序，以及侵害他人名誉、隐私、知识产权和其他合法权益等活动。

**第十三条：**国家支持研究开发有利于未成年人健康成长的网络产品和服务，依法惩治利用网络从事危害未成年人身心健康的活动，为未成年人提供安全、健康的网络环境。

**第十四条：**任何个人和组织有权对危害网络安全的行为向网信、电信、公安等部门举报。收到举报的部门应当及时依法作出处理；不属于本部门职责的，应当及时移送有权处理的部门。

有关部门应当对举报人的相关信息予以保密，保护举报人的合法权益。

## 第二章：网络安全支持与促进

**第十五条：**国家建立和完善网络安全标准体系。国务院标准化行政主管部门和国务院其他有关部门根据各自的职责，组织制定并适时修订有关网络安全管理以及网络产品、服务和运行安全的国家标准、行业标准。

国家支持企业、研究机构、高等学校、网络相关行业组织参与网络安全国家标准、行业标准的制定。

**第十六条：**国务院和省、自治区、直辖市人民政府应当统筹规划，加大投入，扶持重点网络安全技术产业和项目，支持网络安全技术的研究开发和应用，推广安全可信的网络产品和服务，保护网络技术知识产权，支持企业、研究机构 and 高等学校等参与国家网络安全技术创新项目。

**第十七条：**国家推进网络安全社会化服务体系建设，鼓励有关企业、机构开展网络安全认证、检测和风险评估等安全服务。

**第十八条：**国家鼓励开发网络数据安全保护和利用技术，促进公共数据资源开放，推动技术创新和经济社会发展。

国家支持创新网络安全管理方式，运用网络新技术，提升网络安全保护水平。

---

**第十九条：**各级人民政府及其有关部门应当组织开展经常性的网络安全宣传教育，并指导、督促有关单位做好网络安全宣传教育工作。

大众传播媒介应当有针对性地面向社会进行网络安全宣传教育。

**第二十条：**国家支持企业和高等学校、职业学校等教育培训机构开展网络安全相关教育与培训，采取多种方式培养网络安全人才，促进网络安全人才交流。

## 第三章：网络运行安全

### 第一节：一般规定

**第二十一条：**国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：

（一）制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；

（二）采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施；

（三）采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；

（四）采取数据分类、重要数据备份和加密等措施；

（五）法律、行政法规规定的其他义务。

**第二十二条：**网络产品、服务应当符合相关国家标准的强制性要求。网络产品、服务的提供者不得设置恶意程序；发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

网络产品、服务的提供者应当为其产品、服务持续提供安全维护；在规定或者当事人约定的期限内，不得终止提供安全维护。

网络产品、服务具有收集用户信息功能的，其提供者应当向用户明示并取得同意；涉及用户个人信息的，还应当遵守本法和有关法律、行政法规关于个人信息保护的规定。

**第二十三条：**网络关键设备和网络安全专用产品应当按照相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求后，方可销售或者提供。国家网信部门会同国务院有关部门制定、公布网络关键设备和网络安全专用产品目录，并推动安全认证和安全检测结果互认，避免重复认证、检测。

**第二十四条：**网络运营者为用户办理网络接入、域名注册服务，办理固定电话、移动电话等入网手续，或者为用户提供信息发布、即时通讯等服务，在与用户签订协议或者确认提供服务时，应当要求用户提供真实身份信息。用户不提供真实身份信息的，网络运营者不得为其提供相关服务。

国家实施网络可信身份战略，支持研究开发安全、方便的电子身份认证技术，推动不同电子身份认证之间的互认。

**第二十五条：**网络运营者应当制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险；在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告。

**第二十六条：**开展网络安全认证、检测、风险评估等活动，向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息，应当遵守国家有关规定。

**第二十七条：**任何个人和组织不得从事非法侵入他人网络、干扰他人网络正常功能、窃取网络数据等危害网络安全的活动；不得提供专门用于从事侵入网络、干扰网络正常功能及防护措施、窃取网络数据等危害网络安全活动的程序、工具；明知他人从事危害网络安全的活动的，不得为其提供技术支持、广告推广、支付结算等帮助。

**第二十八条：**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。

**第二十九条：**国家支持网络运营者之间在网络安全信息收集、分析、通报和应急处置等方面进行合作，提高网络运营者的安全保障能力。

有关行业组织建立健全本行业的网络安全保护规范和协作机制，加强对网络安全风险的分析评估，定期向会员进行风险警示，支持、协助会员应对网络安全风险。

**第三十条：**网信部门和有关部门在履行网络安全保护职责中获取的信息，只能用于维护网络安全的需要，不得用于其他用途。

## 第二节：关键信息基础设施的运行安全

**第三十一条：**国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。关键信息基础设施的具体范围和安全保护办法由国务院制定。

国家鼓励关键信息基础设施以外的网络运营者自愿参与关键信息基础设施保护体系。

**第三十二条：**按照国务院规定的职责分工，负责关键信息基础设施安全保护工作的部门分别编制并组织实施本行业、本领域的关键信息基础设施安全规划，指导和监督关键信息基础设施运行安全保护工作。

**第三十三条：**建设关键信息基础设施应当确保其具有支持业务稳定、持续运行的性能，并保证安全技术措施同步规划、同步建设、同步使用。

**第三十四条：**除本法第二十一条的规定外，关键信息基础设施的运营者还应当履行下列安全保护义务：

（一）设置专门安全管理机构和安全管理负责人，并对该负责人和关键岗位的人员进行安全背景审查；

（二）定期对从业人员进行网络安全教育、技术培训和技能考核；

（三）对重要系统和数据库进行容灾备份；

（四）制定网络安全事件应急预案，并定期进行演练；

（五）法律、行政法规规定的其他义务。

**第三十五条：**关键信息基础设施的运营者采购网络产品和服务，可能影响国家安全的，应当通过国家网信部门会同国务院有关部门组织的国家安全审查。

**第三十六条：**关键信息基础设施的运营者采购网络产品和服务，应当按照规定与提供者签订安全保密协议，明确安全和保密义务与责任。

**第三十七条：**关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定。

**第三十八条：**关键信息基础设施的运营者应当自行或者委托网络安全服务机构对其网络的安全性和可能存在的风险每年至少进行一次检测评估，并将检测评估情况和改进措施报送相关负责关键信息基础设施安全保护工作的部门。

**第三十九条：**国家网信部门应当统筹协调有关部门对关键信息基础设施的安全保护采取下列措施：

（一）对关键信息基础设施的安全风险进行抽查检测，提出改进措施，必要时可以委托网络安全服务机构对网络存在的安全风险进行检测评估；

（二）定期组织关键信息基础设施的运营者进行网络安全应急演练，提高应对网络安全事件的水平和协同配合能力；

（三）促进有关部门、关键信息基础设施的运营者以及有关研究机构、网络安全服务机构等之间的网络安全信息共享；

（四）对网络安全事件的应急处置与网络功能的恢复等，提供技术支持和协助。

## 第四章：网络信息安全

**第四十条：**网络运营者应当对其收集的用户信息严格保密，并建立健全用户信息保护制度。

**第四十一条：**网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。

网络运营者不得收集与其提供的服务无关的个人信息，不得违反法律、行政法规的规定和双方的约定收集、使用个人信息，并应当依照法律、行政法规的规定和与用户的约定，处理其保存的个人信息。

**第四十二条：**网络运营者不得泄露、篡改、毁损其收集的个人信息；未经被收集者同意，不得向他人提供个人信息。但是，经过处理无法识别特定个人且不能复原的除外。

网络运营者应当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，防止信息泄露、毁损、丢失。在发生或者可能发生个人信息泄露、毁损、丢失的情况时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

**第四十三条：**个人发现网络运营者违反法律、行政法规的规定或者双方的约定收集、使用其个人信息的，有权要求网络运营者删除其个人信息；发现网络运营者收集、存储的其个人信息有错误的，有权要求网络运营者予以更正。网络运营者应当采取措施予以删除或者更正。

**第四十四条：**任何个人和组织不得窃取或者以其他非法方式获取个人信息，不得非法出售或者非法向他人提供个人信息。

**第四十五条：**依法负有网络安全监督管理职责的部门及其工作人员，必须对在履行职责中知悉的个人信息、隐私和商业秘密严格保密，不得泄露、出售或者非法向他人提供。

**第四十六条：**任何个人和组织应当对其使用网络的行为负责，不得设立用于实施诈骗，传授犯罪方法，制作或者销售违禁物品、管制物品等违法犯罪活动的网站、通讯群组，不得利用网络发布涉及实施诈骗，制作或者销售违禁物品、管制物品以及其他违法犯罪活动的信息。

**第四十七条：**网络运营者应当加强对其用户发布的信息的管理，发现法律、行政法规禁止发布或者传输的信息的，应当立即停止传输该信息，采取消除等处置措施，防止信息扩散，保存有关记录，并向有关主管部门报告。

**第四十八条：**任何个人和组织发送的电子信息、提供的应用软件，不得设置恶意程序，不得含有法律、行政法规禁止发布或者传输的信息。

电子信息发送服务提供者 and 应用软件下载服务提供者，应当履行安全管理义务，知道其用户有前款规定行为的，应当停止提供服务，采取消除等处置措施，保存有关记录，并向有关主管部门报告。

**第四十九条：**网络运营者应当建立网络信息安全投诉、举报制度，公布投诉、举报方式等信息，及时受理并处理有关网络信息安全的投诉和举报。

网络运营者对网信部门和有关部门依法实施的监督检查，应当予以配合。

**第五十条：**国家网信部门和有关部门依法履行网络信息安全监督管理职责，发现法律、行政法规禁止发布或者传输的信息的，应当要求网络运营者停止传输，采取消除等处置措施，保存有关记录；对来源于中华人民共和国境外的上述信息，应当通知有关机构采取技术措施和其他必要措施阻断传播。

## 第五章：监测预警与应急处置

**第五十一条：**国家建立网络安全监测预警和信息通报制度。国家网信部门应当统筹协调有关部门加强网络安全信息收集、分析和通报工作，按照规定统一发布网络安全监测预警信息。

**第五十二条：**负责关键信息基础设施安全保护工作的部门，应当建立健全本行业、本领域的网络安全监测预警和信息通报制度，并按照规定报送网络安全监测预警信息。

**第五十三条：**国家网信部门协调有关部门建立健全网络安全风险评估和应急工作机制，制定网络安全事件应急预案，并定期组织演练。

负责关键信息基础设施安全保护工作的部门应当制定本行业、本领域的网络安全事件应急预案，并定期组织演练。

网络安全事件应急预案应当按照事件发生后的危害程度、影响范围等因素对网络安全事件进行分级，并规定相应的应急处置措施。

**第五十四条：**网络安全事件发生的风险增大时，省级以上人民政府有关部门应当按照规定的权限和程序，并根据网络安全风险的特点和可能造成的危害，采取下列措施：

（一）要求有关部门、机构和人员及时收集、报告有关信息，加强对网络安全风险的监测；

（二）组织有关部门、机构和专业人员，对网络安全风险信息进行分析评估，预测事件发生的可能性、影响范围和危害程度；

（三）向社会发布网络安全风险预警，发布避免、减轻危害的措施。

**第五十五条：**发生网络安全事件，应当立即启动网络安全事件应急预案，对网络安全事件进行调查和评估，要求网络运营者采取技术措施和其他必要措施，消除安全隐患，防止危害扩大，并及时向社会发布与公众有关的警示信息。

**第五十六条：**省级以上人民政府有关部门在履行网络安全监督管理职责中，发现网络存在较大安全风险或者发生安全事件的，可以按照规定的权限和程序对该网络的运营者的法定代表人或者主要负责人进行约谈。网络运营者应当按照要求采取措施，进行整改，消除隐患。

**第五十七条：**因网络安全事件，发生突发事件或者生产安全事故的，应当依照《中华人民共和国突发事件应对法》、《中华人民共和国安全生产法》等有关法律、行政法规的规定处置。

**第五十八条：**因维护国家安全和社会公共秩序，处置重大突发社会安全事件的需要，经国务院决定或者批准，可以在特定区域对网络通信采取限制等临时措施。

## 第六章：法律责任

**第五十九条：**网络运营者不履行本法第二十一条、第二十五条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处一万元以上十万元以下罚款，对直接负责的主管人员处五千元以上五万元以下罚款。

关键信息基础设施的运营者不履行本法第三十三条、第三十四条、第三十六条、第三十八条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。

**第六十条：**违反本法第二十二条第一款、第二款和第四十八条第一款规定，有下列行为之一的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处五万元以上五十万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款：

（一）设置恶意程序的；

（二）对其产品、服务存在的安全缺陷、漏洞等风险未立即采取补救措施，或者未按照规定及时告知用户并向有关主管部门报告的；

（三）擅自终止为其产品、服务提供安全维护的。

**第六十一条：**网络运营者违反本法第二十四条第一款规定，未要求用户提供真实身份信息，或者对不提供真实身份信息的用户提供相关服务的，由有关主管部门责令改正；拒不改正或者情节严重的，处五万元以上五十万元以下罚款，并可以由有关主管部门责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

**第六十二条：**违反本法第二十六条规定，开展网络安全认证、检测、风险评估等活动，或者向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息的，由有关主管部门责令改正，给予警告；拒不改正或者情节严重的，处一万元以上十万元以下罚款，并可以由有关主管部门责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处五千元以上五万元以下罚款。

**第六十三条：**违反本法第二十七条规定，从事危害网络安全的活动，或者提供专门用于从事危害网络安全活动的程序、工具，或者为他人从事危害网络安全的活动提供技术支持、广告推广、支付结算等帮助，尚不构成犯罪的，由公安机关没收违法所得，处五日以下拘留，可以并处五万元以上五十万元以下罚款；情节严重的，处五日以上十五日以下拘留，可以并处十万元以上一百万元以下罚款。



---

单位有前款行为的，由公安机关没收违法所得，处十万元以上一百万元以下罚款，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。

违反本法第二十七条规定，受到治安管理处罚的人员，五年内不得从事网络安全管理和网络运营关键岗位的工作；受到刑事处罚的人员，终身不得从事网络安全管理和网络运营关键岗位的工作。

**第六十四条：**网络运营者、网络产品或者服务的提供者违反本法第二十二条第三款、第四十一条至第四十三条规定，侵害个人信息依法得到保护的权利的，由有关主管部门责令改正，可以根据情节单处或者并处警告、没收违法所得、处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款；情节严重的，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照。

违反本法第四十四条规定，窃取或者以其他非法方式获取、非法出售或者非法向他人提供个人信息，尚不构成犯罪的，由公安机关没收违法所得，并处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款。

**第六十五条：**关键信息基础设施的运营者违反本法第三十五条规定，使用未经安全审查或者安全审查未通过的网络产品或者服务的，由有关主管部门责令停止使用，处采购金额一倍以上十倍以下罚款；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

**第六十六条：**关键信息基础设施的运营者违反本法第三十七条规定，在境外存储网络数据，或者向境外提供网络数据的，由有关主管部门责令改正，给予警告，没收违法所得，处五万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

**第六十七条：**违反本法第四十六条规定，设立用于实施违法犯罪活动的网站、通讯群组，或者利用网络发布涉及实施违法犯罪活动的信息，尚不构成犯罪的，由公安机关处五日以下拘留，可以并处一万元以上十万元以下罚款；情节较重的，处五日以上十五日以下拘留，可以并处五万元以上五十万元以下罚款。关闭用于实施违法犯罪活动的网站、通讯群组。

单位有前款行为的，由公安机关处十万元以上五十万元以下罚款，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。

**第六十八条：**网络运营者违反本法第四十七条规定，对法律、行政法规禁止发布或者传输的信息未停止传输、采取消除等处置措施、保存有关记录的，由有关主管部门责令改正，给予警告，没收违法所得；拒不改正或者情节严重的，处十万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

电子信息发送服务提供者、应用软件下载服务提供者，不履行本法第四十八条第二款规定的安全管理义务的，依照前款规定处罚。

**第六十九条：**网络运营者违反本法规定，有下列行为之一的，由有关主管部门责令改正；拒不改正或者情节严重的，处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员，处一万元以上十万元以下罚款：

（一）不按照有关部门的要求对法律、行政法规禁止发布或者传输的信息，采取停止传输、消除等处置措施的；

（二）拒绝、阻碍有关部门依法实施的监督检查的；

（三）拒不向公安机关、国家安全机关提供技术支持和协助的。

**第七十条：**发布或者传输本法第十二条第二款和其他法律、行政法规禁止发布或者传输的信息的，依照有关法律、行政法规的规定处罚。

**第七十一条：**有本法规定的违法行为的，依照有关法律、行政法规的规定记入信用档案，并予以公示。

**第七十二条：**国家机关政务网络的运营者不履行本法规定的网络安全保护义务的，由其上级机关或者有关机关责令改正；对直接负责的主管人员和其他直接责任人员依法给予处分。

**第七十三条：**网信部门和有关部门违反本法第三十条规定，将在履行网络安全保护职责中获取的信息用于其他用途的，对直接负责的主管人员和其他直接责任人员依法给予处分。

网信部门和有关部门的工作人员玩忽职守、滥用职权、徇私舞弊，尚不构成犯罪的，依法给予处分。

**第七十四条：**违反本法规定，给他人造成损害的，依法承担民事责任。

违反本法规定，构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

**第七十五条：**境外的机构、组织、个人从事攻击、侵入、干扰、破坏等危害中华人民共和国的关键信息基础设施的活动，造成严重后果的，依法追究法律责任；国务院公安部门和有关部门并可以决定对该机构、组织、个人采取冻结财产或者其他必要的制裁措施。

## 第七章：附则

**第七十六条：**本法下列用语的含义：

（一）网络，是指由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的系统。

（二）网络安全，是指通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

（三）网络运营者，是指网络的所有者、管理者和网络服务提供者。

（四）网络数据，是指通过网络收集、存储、传输、处理和产生的各种电子数据。

（五）个人信息，是指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。

**第七十七条：**存储、处理涉及国家秘密信息的网络的运行安全保护，除应当遵守本法外，还应当遵守保密法律、行政法规的规定。

**第七十八条：**军事网络的安全保护，由中央军事委员会另行规定。

**第七十九条：**本法自 2017 年 6 月 1 日起施行。

## 附录 2

### 工业和信息化部互联网域名管理办法<sup>31</sup>（节选）

本办法**第三条**规定：工业和信息化部“对全国的域名服务实施监督管理，主要职责是：（一）制定互联网域名管理规章及政策；（二）制定中国互联网域名体系、域名资源发展规划；（三）管理境内的域名根服务器运行机构和域名注册管理机构；（四）负责域名体系的网络与信息安全管理；（五）依法保护用户个人信息和合法权益；（六）负责与域名有关的国际协调；（七）管理境内的域名解析服务；（八）管理其他与域名服务相关的活动。”

本办法**第十条**规定：“申请设立域名根服务器及域名根服务器运行机构的，应当具备以下条件：

（一）域名根服务器设置在境内，并且符合互联网发展相关规划及域名系统安全稳定运行要求。”

**第十一条**：申请设立域名注册管理机构的，应当具备以下条件：

（一）域名管理系统设置在境内，并且持有的顶级域名符合相关法律法规及域名系统安全稳定运行要求；

（二）是依法设立的法人，该法人及其主要出资者、主要经营管理人员具有良好的信用记录；

（三）具有完善的业务发展计划和技术方案以及与从事顶级域名运行管理相适应的场地、资金、专业人员以及符合电信管理机构要求的信息管理系统；

（四）具有健全的网络与信息安全保障措施，包括管理人员、网络与信息安全管理制度、应急处置预案和相关技术、管理措施等；

（五）具有进行真实身份信息核验和用户个人信息保护的能力、提供长期服务的能力及健全的服务退出机制；

（六）具有健全的域名注册服务管理制度和对域名注册服务机构的监督机制；

（七）法律、行政法规规定的其他条件。

**第十二条**：申请设立域名注册服务机构的，应当具备以下条件：

（一）在境内设置域名注册服务系统、注册数据库和相应的域名解析系统；

（二）是依法设立的法人，该法人及其主要出资者、主要经营管理人员具有良好的信用记录；

（三）具有与从事域名注册服务相适应的场地、资金和专业人员以及符合电信管理机构要求的信息管理系统；

（四）具有进行真实身份信息核验和用户个人信息保护的能力、提供长期服务的能力及健全的服务退出机制；

（五）具有健全的域名注册服务管理制度和对域名注册代理机构的监督机制；

（六）具有健全的网络与信息安全保障措施，包括管理人员、网络与信息安全管理制度、应急处置预案和相关技术、管理措施等。

（七）法律、行政法规规定的其他条件。

**第十三条**：申请设立域名根服务器及域名根服务器运行机构、域名注册管理机构的，应当向工业和信息化部提交申请材料。申请设立域名注册服务机构的，应当向住所地省、自治区、直辖市通信管理局提交申请材料。

<sup>31</sup> 工业和信息化部，《互联网域名管理办法》，2017年8月24日：[http://www.cac.gov.cn/2017-09/28/c\\_1121737753.htm](http://www.cac.gov.cn/2017-09/28/c_1121737753.htm)，非官方英文翻译链接：<https://www.chinalawtranslate.com/en/internet-domain-name-management-measures/>。

---

申请材料应当包括：

- （一）申请单位的基本情况；
- （二）对域名服务实施有效管理的证明材料，包括相关系统及场所、服务能力的证明材料、管理制度、与其他机构签订的协议等；
- （三）网络与信息安全保障制度及措施；
- （四）证明申请单位信誉的材料；
- （五）法定代表人签署的依法诚信经营承诺书。

**第三十七条：**“提供域名解析服务，不得擅自篡改解析信息。任何组织或者个人不得恶意将域名解析指向他人的 IP 地址。”

本办法**第四十一条**规定：“因国家安全和处置紧急事件的需要，域名根服务器运行机构、域名注册管理机构和域名注册服务机构应当服从电信管理机构的统一指挥与协调，遵守电信管理机构的管理要求。”

**第四十六条：**“电信管理机构应当建立域名根服务器运行机构、域名注册管理机构和域名注册服务机构的信用记录制度，将其违反本办法并受到行政处罚的行为记入信用档案。”

---

## 附录 3

### 中国互联网域名体系<sup>32</sup>（节选）

一、我国互联网域名体系中各级域名可以由字母（A-Z，a-z，大小写等效）、数字（0-9）、连接符（-）或汉字组成，各级域名之间用实点（.）连接，中文域名的各级域名之间用实点或中文句号（。）连接。

二、我国互联网域名体系在国家顶级域名“.CN”“.中国”之外，设有多个英文和中文顶级域名，其中“.政务”“.公益”顶级域名为面向我国党政群机关等各级政务部门及非营利性机构的专用中文顶级域名。我国互联网域名体系图详见“<http://中国互联网域名体系.中国>”“<http://中国互联网域名体系.政务>”或“<http://中国互联网域名体系.信息>”。

三、国家顶级域名“.CN”之下，设置“类别域名”和“行政区域名”两类二级域名。设置“类别域名”9个，分别为：“政务”适用于党政群机关等各级政务部门；“公益”适用于非营利性机构；“GOV”适用于政府机构；“ORG”适用于非营利性的组织；“AC”适用于科研机构；“COM”适用于工、商、金融等企业；“EDU”适用于教育机构；“MIL”适用于国防机构；“NET”适用于提供互联网服务的机构。

设置“行政区域名”34个，适用于我国的各省、自治区、直辖市、特别行政区的组织[...]

四、在国家顶级域名“.CN”“.中国”下可以直接申请注册二级域名。

---

<sup>32</sup>中国法律翻译网，《中国互联网域名体系》，2018年3月5日，非官方英文翻译链接：  
<https://www.chinalawtranslate.com/en/chinese-internet-domain-name-system/>。

## 附录 4

### 中华人民共和国数据安全法<sup>33</sup>（节选）

**第三条：**本法所称数据，是指任何以电子或者其他方式对信息的记录。

数据处理，包括数据的收集、存储、使用、加工、传输、提供、公开等。

数据安全，是指通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

**第七条：**国家保护个人、组织与数据有关的权益，鼓励数据依法合理有效利用，保障数据依法有序自由流动，促进以数据为关键要素的数字经济发展。

**第十一条：**国家积极开展数据安全治理、数据开发利用等领域的国际交流与合作，参与数据安全相关国际规则和标准的制定，促进数据跨境安全、自由流动。

**第十四条：**国家实施大数据战略，推进数据基础设施建设，鼓励和支持数据在各行业、各领域的创新应用。

**第十七条：**国家推进数据开发利用技术和数据安全标准体系建设。国务院标准化行政主管部门和国务院有关部门根据各自的职责，组织制定并适时修订有关数据开发利用技术、产品和数据安全相关标准。国家支持企业、社会团体和教育、科研机构等参与标准制定。

**第二十一条：**关系国家安全、国民经济命脉、重要民生、重大公共利益等数据属于国家核心数据，实行更加严格的管理制度。

**第二十五条：**国家对与维护国家安全和利益、履行国际义务相关的属于管制物项的数据依法实施出口管制。

**第二十六条：**任何国家或者地区在与数据和数据开发利用技术等有关的投资、贸易等方面对中华人民共和国采取歧视性的禁止、限制或者其他类似措施的，中华人民共和国可以根据实际情况对该国家或者地区对等采取措施。

**第二十七条：**利用互联网等信息网络开展数据处理活动，应当在网络安全等级保护制度的基础上，履行上述数据安全保护义务。

**第三十一条：**关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的重要数据的出境安全管理，适用《中华人民共和国网络安全法》的规定；其他数据处理者在中华人民共和国境内运营中收集和产生的重要数据的出境安全管理办法，由国家网信部门会同国务院有关部门制定。

**第三十二条：**任何组织、个人收集数据，应当采取合法、正当的方式，不得窃取或者以其他非法方式获取数据。法律、行政法规对收集、使用数据的目的、范围有规定的，应当在法律、行政法规规定的目的和范围内收集、使用数据。

<sup>33</sup> 《中华人民共和国数据安全法》，2021年6月11日：[http://www.cac.gov.cn/2021-06/11/c\\_1624994566919140.htm](http://www.cac.gov.cn/2021-06/11/c_1624994566919140.htm)，非官方英文翻译链接：<https://www.secrss.com/articles/31844>。

---

**第三十三条：**从事数据交易中介服务的机构提供服务，应当要求数据提供方说明数据来源，审核交易双方的身份，并留存审核、交易记录。

**第三十六条：**中华人民共和国主管机关根据有关法律和中华人民共和国缔结或者参加的国际条约、协定，或者按照平等互惠原则，处理外国司法或者执法机构关于提供数据的请求。非经中华人民共和国主管机关批准，境内的组织、个人不得向外国司法或者执法机构提供存储于中华人民共和国境内的数据。

**第三十八条：**国家机关为履行法定职责的需要收集、使用数据，应当在其履行法定职责的范围内依照法律、行政法规规定的条件和程序进行；对在履行职责中知悉的个人隐私、个人信息、商业秘密、保密商务信息等数据应当依法予以保密，不得泄露或者非法向他人提供。

**第四十条：**国家机关委托他人建设、维护电子政务系统，存储、加工政务数据，应当经过严格的批准程序，并应当监督受托方履行相应的数据安全保护义务。受托方应当依照法律、法规的规定和合同约定履行数据安全保护义务，不得擅自留存、使用、泄露或者向他人提供政务数据。

**第四十四条：**有关主管部门在履行数据安全监管职责中，发现数据处理活动存在较大安全风险的，可以按照规定的权限和程序对有关组织、个人进行约谈，并要求有关组织、个人采取措施进行整改，消除隐患。

**第四十九条：**国家机关不履行本法规定的数据安全保护义务的，对直接负责的主管人员和其他直接责任人员依法给予处分。

**第五十二条：**违反本法规定，给他人造成损害的，依法承担民事责任。

---

## 附录 5

### 中华人民共和国个人信息保护法<sup>34</sup>

(2021年8月20日第十三届全国人民代表大会常务委员会第三十次会议通过)

第一章：总则

第二章：个人信息处理规则

第一节：一般规定

第二节：敏感个人信息的处理规则

第三节：国家机关处理个人信息的特别规定

第三章：个人信息跨境提供的规则

第四章：个人在个人信息处理活动中的权利

第五章：个人信息处理者的义务

第六章：履行个人信息保护职责的部门

第七章：法律责任

第八章：附则

#### 第一章：总则

**第一条：**为了保护个人信息权益，规范个人信息处理活动，促进个人信息合理利用，根据宪法，制定本法。

**第二条：**自然人的个人信息受法律保护，任何组织、个人不得侵害自然人的个人信息权益。

**第三条：**在中华人民共和国境内处理自然人个人信息的活动，适用本法。

在中华人民共和国境外处理中华人民共和国境内自然人个人信息的活动，有下列情形之一的，也适用本法：

- (一) 以向境内自然人提供产品或者服务为目的；
- (二) 分析、评估境内自然人的行为；
- (三) 法律、行政法规规定的其他情形。

**第四条：**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。

个人信息的处理包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等。

**第五条：**处理个人信息应当遵循合法、正当、必要和诚信原则，不得通过误导、欺诈、胁迫等方式处理个人信息。

**第六条：**处理个人信息应当具有明确、合理的目的，并应当与处理目的直接相关，采取对个人权益影响最小的方式。

收集个人信息，应当限于实现处理目的的最小范围，不得过度收集个人信息。

---

<sup>34</sup> 《中华人民共和国个人信息保护法》，（2021年8月20日第十三届全国人民代表大会常务委员会第三十次会议通过），<http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml>，非官方英文翻译链接：<https://digichina.stanford.edu/news/translation-personal-information-protection-law-peoples-republic-china-effective-nov-1-2021>。



**第七条：**处理个人信息应当遵循公开、透明原则，公开个人信息处理规则，明示处理的目的、方式和范围。

**第八条：**处理个人信息应当保证个人信息的质量，避免因个人信息不准确、不完整对个人权益造成不利影响。

**第九条：**个人信息处理者应当对其个人信息处理活动负责，并采取必要措施保障所处理的个人信息的安全。

**第十条：**任何组织、个人不得非法收集、使用、加工、传输他人个人信息，不得非法买卖、提供或者公开他人个人信息；不得从事危害国家安全、公共利益的个人信息处理活动。

**第十一条：**国家建立健全个人信息保护制度，预防和惩治侵害个人信息权益的行为，加强个人信息保护宣传教育，推动形成政府、企业、相关社会组织、公众共同参与个人信息保护的良好环境。

**第十二条：**国家积极参与个人信息保护国际规则的制定，促进个人信息保护方面的国际交流与合作，推动与其他国家、地区、国际组织之间的个人信息保护规则、标准等互认。

## 第二章：个人信息处理规则

### 第一节：一般规定

**第十三条：**符合下列情形之一的，个人信息处理者方可处理个人信息：

（一）取得个人的同意；

（二）为订立、履行个人作为一方当事人的合同所必需，或者按照依法制定的劳动规章制度和依法签订的集体合同实施人力资源管理所必需；

（三）为履行法定职责或者法定义务所必需；

（四）为应对突发公共卫生事件，或者紧急情况下为保护自然人的生命健康和财产安全所必需；

（五）为公共利益实施新闻报道、舆论监督等行为，在合理的范围内处理个人信息；

（六）依照本法规定在合理的范围内处理个人自行公开或者其他已经合法公开的个人信息；

（七）法律、行政法规规定的其他情形。

依照本法其他有关规定，处理个人信息应当取得个人同意。但是有前款第二项至第七项规定情形的，不需取得个人同意。

**第十四条：**基于个人同意处理个人信息的，该同意应当由个人在充分知情的前提下自愿、明确作出。法律、行政法规规定处理个人信息应当取得个人单独同意或者书面同意的，从其规定。

个人信息的处理目的、处理方式和处理的个人信息种类发生变更的，应当重新取得个人同意。

**第十五条：**基于个人同意处理个人信息的，个人有权撤回其同意。个人信息处理者应当提供便捷的撤回同意的方式。

个人撤回同意，不影响撤回前基于个人同意已进行的个人信息处理活动的效力。

**第十六条：**个人信息处理者不得以个人不同意处理其个人信息或者撤回同意为由，拒绝提供产品或者服务；处理个人信息属于提供产品或者服务所必需的除外。

**第十七条：**个人信息处理者在处理个人信息前，应当以显著方式、清晰易懂的语言真实、准确、完整地向个人告知下列事项：

- （一）个人信息处理者的名称或者姓名和联系方式；
- （二）个人信息的处理目的、处理方式，处理的个人信息种类、保存期限；
- （三）个人行使本法规定权利的方式和程序；
- （四）法律、行政法规规定应当告知的其他事项。

前款规定事项发生变更的，应当将变更部分告知个人。

个人信息处理者通过制定个人信息处理规则的方式告知第一款规定事项的，处理规则应当公开，并且便于查阅和保存。

**第十八条：**个人信息处理者处理个人信息，有法律、行政法规规定应当保密或者不需要告知的情形的，可以不向个人告知前条第一款规定的事项。

紧急情况下为保护自然人的生命健康和财产安全无法及时向个人告知的，个人信息处理者应当在紧急情况消除后及时告知。

**第十九条：**除法律、行政法规另有规定外，个人信息的保存期限应当为实现处理目的所必要的最短时间。

**第二十条：**两个以上的个人信息处理者共同决定个人信息的处理目的和处理方式的，应当约定各自的权利和义务。但是，该约定不影响个人向其中任何一个个人信息处理者要求行使本法规定的权利。

个人信息处理者共同处理个人信息，侵害个人信息权益造成损害的，应当依法承担连带责任。

**第二十一条：**个人信息处理者委托处理个人信息的，应当与受托人约定委托处理的目的、期限、处理方式、个人信息的种类、保护措施以及双方的权利和义务等，并对受托人的个人信息处理活动进行监督。

受托人应当按照约定处理个人信息，不得超出约定的处理目的、处理方式等处理个人信息；委托合同不生效、无效、被撤销或者终止的，受托人应当将个人信息返还个人信息处理者或者予以删除，不得保留。

未经个人信息处理者同意，受托人不得转委托他人处理个人信息。

**第二十二条：**个人信息处理者因合并、分立、解散、被宣告破产等原因需要转移个人信息的，应当向个人告知接收方的名称或者姓名和联系方式。接收方应当继续履行个人信息处理者的义务。接收方变更原先的处理目的、处理方式的，应当依照本法规定重新取得个人同意。

**第二十三条：**个人信息处理者向其他个人信息处理者提供其处理的个人信息的，应当向个人告知接收方的名称或者姓名、联系方式、处理目的、处理方式和个人信息的种类，并取得个人的单独同意。接收方应当在上述处理目的、处理方式和个人信息的种类等范围内处理个人信息。接收方变更原先的处理目的、处理方式的，应当依照本法规定重新取得个人同意。

**第二十四条：**个人信息处理者利用个人信息进行自动化决策，应当保证决策的透明度和结果公平、公正，不得对个人在交易价格等交易条件上实行不合理的差别待遇。

通过自动化决策方式向个人进行信息推送、商业营销，应当同时提供不针对其个人特征的选项，或者向个人提供便捷的拒绝方式。

通过自动化决策方式作出对个人权益有重大影响的决定，个人有权要求个人信息处理者予以说明，并有权拒绝个人信息处理者仅通过自动化决策的方式作出决定。

---

**第二十五条：**个人信息处理者不得公开其处理的个人信息，取得个人单独同意的除外。

**第二十六条：**在公共场所安装图像采集、个人身份识别设备，应当为维护公共安全所必需，遵守国家有关规定，并设置显著的提示标识。所收集的个人信息、身份识别信息只能用于维护公共安全的目的，不得用于其他目的；取得个人单独同意的除外。

**第二十七条：**个人信息处理者可以在合理的范围内处理个人自行公开或者其他已经合法公开的个人信息；个人明确拒绝的除外。个人信息处理者处理已公开的个人信息，对个人权益有重大影响的，应当依照本法规定取得个人同意。

## 第二节：敏感个人信息的处理规则

**第二十八条：**敏感个人信息是一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。

只有在具有特定的目的和充分的必要性，并采取严格保护措施的情形下，个人信息处理者方可处理敏感个人信息。

**第二十九条：**处理敏感个人信息应当取得个人的单独同意；法律、行政法规规定处理敏感个人信息应当取得书面同意的，从其规定。

**第三十条：**个人信息处理者处理敏感个人信息的，除本法第十七条第一款规定的事项外，还应当向个人告知处理敏感个人信息的必要性以及对个人权益的影响；依照本法规定可以不向个人告知的除外。

**第三十一条：**个人信息处理者处理不满十四周岁未成年人个人信息的，应当取得未成年人的父母或者其他监护人的同意。

个人信息处理者处理不满十四周岁未成年人个人信息的，应当制定专门的个人信息处理规则。

**第三十二条：**法律、行政法规对处理敏感个人信息规定应当取得相关行政许可或者作出其他限制的，从其规定。

## 第三节：国家机关处理个人信息的特别规定

**第三十三条：**国家机关处理个人信息的活动，适用本法；本节有特别规定的，适用本节规定。

**第三十四条：**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。

**第三十五条：**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。

**第三十六条：**国家机关处理的个人信息应当在中华人民共和国境内存储；确需向境外提供的，应当进行安全评估。安全评估可以要求有关部门提供支持协助。

**第三十七条：**法律、法规授权的具有管理公共事务职能的组织为履行法定职责处理个人信息，适用本法关于国家机关处理个人信息的规定。

### 第三章：个人信息跨境提供的规则

**第三十八条：**个人信息处理者因业务等需要，确需向中华人民共和国境外提供个人信息的，应当具备下列条件之一：

- （一）依照本法第四十条的规定通过国家网信部门组织的安全评估；
- （二）按照国家网信部门的规定经专业机构进行个人信息保护认证；
- （三）按照国家网信部门制定的标准合同与境外接收方订立合同，约定双方的权利和义务；
- （四）法律、行政法规或者国家网信部门规定的其他条件。

中华人民共和国缔结或者参加的国际条约、协定对向中华人民共和国境外提供个人信息的条件等有规定的，可以按照其规定执行。

个人信息处理者应当采取必要措施，保障境外接收方处理个人信息的活动达到本法规定的个人信息保护标准。

**第三十九条：**个人信息处理者向中华人民共和国境外提供个人信息的，应当向个人告知境外接收方的名称或者姓名、联系方式、处理目的、处理方式、个人信息的种类以及个人向境外接收方行使本法规定权利的方式和程序等事项，并取得个人的单独同意。

**第四十条：**关键信息基础设施运营者和处理个人信息达到国家网信部门规定数量的个人信息处理者，应当将在中华人民共和国境内收集和产生的个人信息存储在境内。确需向境外提供的，应当通过国家网信部门组织的安全评估；法律、行政法规和国家网信部门规定可以不进行安全评估的，从其规定。

**第四十一条：**中华人民共和国主管机关根据有关法律和中华人民共和国缔结或者参加的国际条约、协定，或者按照平等互惠原则，处理外国司法或者执法机构关于提供存储于境内个人信息的请求。非经中华人民共和国主管机关批准，个人信息处理者不得向外国司法或者执法机构提供存储于中华人民共和国境内的个人信息。

**第四十二条：**境外的组织、个人从事侵害中华人民共和国公民的个人信息权益，或者危害中华人民共和国国家安全、公共利益的个人信息的处理活动的，国家网信部门可以将其列入限制或者禁止个人信息提供清单，予以公告，并采取限制或者禁止向其提供个人信息等措施。

**第四十三条：**任何国家或者地区在个人信息保护方面对中华人民共和国采取歧视性的禁止、限制或者其他类似措施的，中华人民共和国可以根据实际情况对该国家或者地区对等采取措施。

### 第四章：个人在个人信息处理活动中的权利

**第四十四条：**个人对其个人信息的处理享有知情权、决定权，有权限制或者拒绝他人对其个人信息进行处理；法律、行政法规另有规定的除外。

**第四十五条：**个人有权向个人信息处理者查阅、复制其个人信息；有本法第十八条第一款、第三十五条规定情形的除外。

个人请求查阅、复制其个人信息的，个人信息处理者应当及时提供。

个人请求将个人信息转移至其指定的个人信息处理者，符合国家网信部门规定条件的，个人信息处理者应当提供转移的途径。

**第四十六条：**个人发现其个人信息不准确或者不完整的，有权请求个人信息处理者更正、补充。个人请求更正、补充其个人信息的，个人信息处理者应当对其个人信息予以核实，并及时更正、补充。

**第四十七条：**有下列情形之一的，个人信息处理者应当主动删除个人信息；个人信息处理者未删除的，个人有权请求删除：

- (一) 处理目的已实现、无法实现或者为实现处理目的不再必要；
- (二) 个人信息处理者停止提供产品或者服务，或者保存期限已届满；
- (三) 个人撤回同意；
- (四) 个人信息处理者违反法律、行政法规或者违反约定处理个人信息；
- (五) 法律、行政法规规定的其他情形。

法律、行政法规规定的保存期限未届满，或者删除个人信息从技术上难以实现的，个人信息处理者应当停止除存储和采取必要的安全保护措施之外的处理。

**第四十八条：**个人有权要求个人信息处理者对其个人信息处理规则进行解释说明。

**第四十九条：**自然人死亡的，其近亲属为了自身的合法、正当利益，可以对死者的相关个人信息行使本章规定的查阅、复制、更正、删除等权利；死者生前另有安排的除外。

**第五十条：**个人信息处理者应当建立便捷的个人行使权利的申请受理和处理机制。拒绝个人行使权利的请求的，应当说明理由。

个人信息处理者拒绝个人行使权利的请求的，个人可以依法向人民法院提起诉讼。

## 第五章：个人信息处理者的义务

**第五十一条：**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：

- (一) 制定内部管理制度和操作规程；
- (二) 对个人信息实行分类管理；
- (三) 采取相应的加密、去标识化等安全技术措施；
- (四) 合理确定个人信息处理的操作权限，并定期对从业人员进行安全教育和培训；
- (五) 制定并组织实施个人信息安全事件应急预案；
- (六) 法律、行政法规规定的其他措施。

**第五十二条：**处理个人信息达到国家网信部门规定数量的个人信息处理者应当指定个人信息保护负责人，负责对个人信息处理活动以及采取的保护措施等进行监督。

个人信息处理者应当公开个人信息保护负责人的联系方式，并将个人信息保护负责人的姓名、联系方式等报送履行个人信息保护职责的部门。

**第五十三条：**本法第三条第二款规定的中华人民共和国境外的个人信息处理者，应当在中华人民共和国境内设立专门机构或者指定代表，负责处理个人信息保护相关事务，并将有关机构的名称或者代表的姓名、联系方式等报送履行个人信息保护职责的部门。

**第五十四条：**个人信息处理者应当定期对其处理个人信息遵守法律、行政法规的情况进行合规审计。

**第五十五条：**有下列情形之一的，个人信息处理者应当事前进行个人信息保护影响评估，并对处理情况进行记录：

- (一) 处理敏感个人信息；
- (二) 利用个人信息进行自动化决策；
- (三) 委托处理个人信息、向其他个人信息处理者提供个人信息、公开个人信息；
- (四) 向境外提供个人信息；
- (五) 其他对个人权益有重大影响的个人信息处理活动。

**第五十六条：**个人信息保护影响评估应当包括下列内容：

- (一) 个人信息的处理目的、处理方式等是否合法、正当、必要；
- (二) 对个人权益的影响及安全风险；
- (三) 所采取的保护措施是否合法、有效并与风险程度相适应。

个人信息保护影响评估报告和处理情况记录应当至少保存三年。

**第五十七条：**发生或者可能发生个人信息泄露、篡改、丢失的，个人信息处理者应当立即采取补救措施，并通知履行个人信息保护职责的部门和个人。通知应当包括下列事项：

- (一) 发生或者可能发生个人信息泄露、篡改、丢失的信息种类、原因和可能造成的危害；
- (二) 个人信息处理者采取的补救措施和个人可以采取的减轻危害的措施；
- (三) 个人信息处理者的联系方式。

个人信息处理者采取措施能够有效避免信息泄露、篡改、丢失造成危害的，个人信息处理者可以不通知个人；履行个人信息保护职责的部门认为可能造成危害的，有权要求个人信息处理者通知个人。

**第五十八条：**提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者，应当履行下列义务：

- (一) 按照国家规定建立健全个人信息保护合规制度体系，成立主要由外部成员组成的独立机构对个人信息保护情况进行监督；
- (二) 遵循公开、公平、公正的原则，制定平台规则，明确平台内产品或者服务提供者处理个人信息的规范和保护个人信息的义务；
- (三) 对严重违反法律、行政法规处理个人信息的平台内的产品或者服务提供者，停止提供服务；
- (四) 定期发布个人信息保护社会责任报告，接受社会监督。

**第五十九条：**接受委托处理个人信息的受托人，应当依照本法和有关法律、行政法规的规定，采取必要措施保障所处理的个人信息的安全，并协助个人信息处理者履行本法规定的义务。

## 第六章：履行个人信息保护职责的部门

**第六十条：**国家网信部门负责统筹协调个人信息保护工作和相关监督管理工作。国务院有关部门依照本法和有关法律、行政法规的规定，在各自职责范围内负责个人信息保护和监督管理工作。县级以上地方人民政府有关部门的个人信息保护和监督管理职责，按照国家有关规定确定。前两款规定的部门统称为履行个人信息保护职责的部门。

**第六十一条：**履行个人信息保护职责的部门履行下列个人信息保护职责：

- (一) 开展个人信息保护宣传教育，指导、监督个人信息处理者开展个人信息保护工作；
- (二) 接受、处理与个人信息保护有关的投诉、举报；
- (三) 组织对应用程序等个人信息保护情况进行测评，并公布测评结果；
- (四) 调查、处理违法个人信息处理活动；
- (五) 法律、行政法规规定的其他职责。

**第六十二条：**国家网信部门统筹协调有关部门依据本法推进下列个人信息保护工作：

- (一) 制定个人信息保护具体规则、标准；
- (二) 针对小型个人信息处理者、处理敏感个人信息以及人脸识别、人工智能等新技术、新应用，制定专门的个人信息保护规则、标准；
- (三) 支持研究开发和推广应用安全、方便的电子身份认证技术，推进网络身份认证公共服务建设；
- (四) 推进个人信息保护社会化服务体系建设，支持有关机构开展个人信息保护评估、认证服务；
- (五) 完善个人信息保护投诉、举报工作机制。

**第六十三条：**履行个人信息保护职责的部门履行个人信息保护职责，可以采取下列措施：

- (一) 询问有关当事人，调查与个人信息处理活动有关的情况；
- (二) 查阅、复制当事人与个人信息处理活动有关的合同、记录、账簿以及其他有关资料；
- (三) 实施现场检查，对涉嫌违法的个人信息处理活动进行调查；
- (四) 检查与个人信息处理活动有关的设备、物品；对有证据证明是用于违法个人信息处理活动的设备、物品，向本部门主要负责人书面报告并经批准，可以查封或者扣押。

履行个人信息保护职责的部门依法履行职责，当事人应当予以协助、配合，不得拒绝、阻挠。

**第六十四条：**履行个人信息保护职责的部门在履行职责中，发现个人信息处理活动存在较大风险或者发生个人信息安全事件的，可以按照规定的权限和程序对该个人信息处理者的法定代表人或者主要负责人进行约谈，或者要求个人信息处理者委托专业机构对其个人信息处理活动进行合规审计。个人信息处理者应当按照要求采取措施，进行整改，消除隐患。

履行个人信息保护职责的部门在履行职责中，发现违法处理个人信息涉嫌犯罪的，应当及时移送公安机关依法处理。

**第六十五条：**任何组织、个人有权对违法个人信息处理活动向履行个人信息保护职责的部门进行投诉、举报。收到投诉、举报的部门应当依法及时处理，并将处理结果告知投诉、举报人。

履行个人信息保护职责的部门应当公布接受投诉、举报的联系方式。

## 第七章：法律责任

**第六十六条：**违反本法规定处理个人信息，或者处理个人信息未履行本法规定的个人信息保护义务的，由履行个人信息保护职责的部门责令改正，给予警告，没收违法所得，对违法处理个人信息的应用程序，责令暂停或者终止提供服务；拒不改正的，并处一百万元以下罚款；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

---

有前款规定的违法行为，情节严重的，由省级以上履行个人信息保护职责的部门责令改正，没收违法所得，并处五千万以下或者上一年度营业额百分之五以下罚款，并可以责令暂停相关业务或者停业整顿、通报有关主管部门吊销相关业务许可或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款，并可以决定禁止其在一定期限内担任相关企业的董事、监事、高级管理人员和个人信息保护负责人。

**第六十七条：**有本法规定的违法行为的，依照有关法律、行政法规的规定记入信用档案，并予以公示。

**第六十八条：**国家机关不履行本法规定的个人信息保护义务的，由其上级机关或者履行个人信息保护职责的部门责令改正；对直接负责的主管人员和其他直接责任人员依法给予处分。

履行个人信息保护职责的部门的工作人员玩忽职守、滥用职权、徇私舞弊，尚不构成犯罪的，依法给予处分。

**第六十九条：**处理个人信息侵害个人信息权益造成损害，个人信息处理者不能证明自己没有过错的，应当承担损害赔偿等侵权责任。

前款规定的损害赔偿按照个人因此受到的损失或者个人信息处理者因此获得的利益确定；个人因此受到的损失和个人信息处理者因此获得的利益难以确定的，根据实际情况确定赔偿数额。

**第七十条：**个人信息处理者违反本法规定处理个人信息，侵害众多个人的权益的，人民检察院、法律规定的消费者组织和由国家网信部门确定的组织可以依法向人民法院提起诉讼。

**第七十一条：**违反本法规定，构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

## 第八章：附则

**第七十二条：**自然人因个人或者家庭事务处理个人信息的，不适用本法。

法律对各级人民政府及其有关部门组织实施的统计、档案管理活动中的个人信息处理有规定的，适用其规定。

**第七十三条：**本法下列用语的含义：

（一）个人信息处理者，是指在个人信息处理活动中自主决定处理目的、处理方式的组织、个人。

（二）自动化决策，是指通过计算机程序自动分析、评估个人的行为习惯、兴趣爱好或者经济、健康、信用状况等，并进行决策的活动。

（三）去标识化，是指个人信息经过处理，使其在不借助额外信息的情况下无法识别特定自然人的过程。

（四）匿名化，是指个人信息经过处理无法识别特定自然人且不能复原的过程。

**第七十四条：**本法自 2021 年 11 月 1 日起施行。



---

## 附录 6

### 关键信息基础设施安全保护条例<sup>35</sup>（节选）

**第二条：**本条例所称关键信息基础设施，是指公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域的，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统等。

**第八条：**本条例第二条涉及的重要行业和领域的主管部门、监督管理部门是负责关键信息基础设施安全保护工作的部门（以下简称保护工作部门）。

**第九条：**保护工作部门结合本行业、本领域实际，制定关键信息基础设施认定规则，并报国务院公安部门备案。

制定认定规则应当主要考虑下列因素：

- （一）网络设施、信息系统等对于本行业、本领域关键核心业务的重要程度；
- （二）网络设施、信息系统等一旦遭到破坏、丧失功能或者数据泄露可能带来的危害程度；
- （三）对其他行业和领域的关联性影响。

**第十八条：**关键信息基础设施发生重大网络安全事件或者发现重大网络安全威胁时，运营者应当按照有关规定向保护工作部门、公安机关报告。

发生关键信息基础设施整体中断运行或者主要功能故障、国家基础信息以及其他重要数据泄露、较大规模个人信息泄露、造成较大经济损失、违法信息较大范围传播等特别重大网络安全事件或者发现特别重大网络安全威胁时，保护工作部门应当在收到报告后，及时向国家网信部门、国务院公安部门报告。

---

<sup>35</sup> 中华人民共和国国务院令 第 745 号，2021 年 7 月 30 日，

[http://www.gov.cn/zhengce/content/2021-08/17/content\\_5631671.htm?trs=1](http://www.gov.cn/zhengce/content/2021-08/17/content_5631671.htm?trs=1)，非官方英文翻译链接：  
<https://digichina.stanford.edu/news/translation-critical-information-infrastructure-security-protection-regulations-effective-sept>。