目　录

草案探析

立法的目的.....1
法规的适用范围.....1
对个人信息定义及其处理的方式.....1
匿名化与去标识化界定.....1
个人信息保护的原则.....2
处理个人信息要事前充分告知取得用户同意.....2
个人信息处理活动中个人权利.....2
对个人信息处理者要求.....2
对境外个人信息处理者的规定.....3
规定敏感个人信息范围.....3
敏感个人信息处理规定.....3
已公开的个人信息处理要求.....3
个人信息的“委托处理关系”的规定.....4
公共场所收集个人身份特征信息的不得随意公开.....4
突发公共卫生事件中要严格保护个人信息.....4
对大数据杀熟、精准推送等自动化决策规定.....4
对删除个人信息的规定.....5
赋予必要域外适用效力.....5
个人信息保护各领域部门的职责分工.....5
相关职能部门履行的保护职责及采取的措施.....6
国家机关处理个人信息的规定.....6
完善个人信息跨境提供规则维护国家安全.....6
草案对违法行为的处罚及民事赔偿规定.....7
简述我国个人信息保护的立法进程.....7

评论分析

个人信息保护法将重点关注哪些方面呢？.....9
个人信息保护法草案值得关注的三大亮点.....9
我们需要一部什么样的个人信息保护法.....10

制定《个人信息保护法》，设置严格的法律责任.....11
国际变局下，个人信息保护立法的5大迫切性.....11
全国政协委员殷兴山建议加快个人信息保护专项立法进程.....12

相关法规

《网络安全法》与个人信息保护.....14
网络安全法中有关个人信息的部分内容.....14
《民法典》时代，个人信息如何保护？.....15
从电子商务法看个人信息保护.....16
《儿童个人信息网络保护规定》亮点解读.....16
《信息安全技术个人信息安全规范》2020版.....17
《数据安全法(草案)》涉及个人信息保护的部分条款.....18

他山之石

国外怎么保护个人信息？.....19
简要认识欧盟最严数据保护法案.....20
综述：欧洲以立法形式保护个人“被遗忘权”.....21

草案探析

《个人信息保护法》草案提请十三届全国人大常委会第二十二次会议审议，共八章七十条，聚焦目前个人信息保护的突出问题。

立法的目的

保护个人信息权益，规范个人信息处理活动，保障个人信息依法有序自由流动，促进个人信息合理利用，制定本法。

法规的适用范围

草案规定，组织、个人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。

草案还规定，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)为分析、评估境内自然人的行为；

(三)法律、行政法规规定的其他情形。

对个人信息定义及其处理的方式

草案明确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、公开等活动。

匿名化与去标识化界定

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。

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。

草案规定**个人信息处理者向第三方提供匿名化信息的，第三方不得利用技术等手段重新识别个人身份。**

个人信息保护的原则

法律草案明确了合法正当、诚信准确、目的明确、知情同意、限制利用、安全保障等几大原则。

草案强调处理个人信息应当采用**合法、正当**的方式，具有明确、合理的目的，限于实现处理目的的最小范围，公开处理规则，保证信息准确，采取安全保护措施等，并将上述原则贯穿于个人信息处理的全过程、各环节。

处理个人信息要事前充分告知取得用户同意

草案中确立了**以“告知—同意”为核心**的个人信息处理规则，即：处理个人信息应当在**事先充分告知的前提下取得个人同意**，并且个人有权撤回同意；重要事项发生变更的应当重新取得个人同意；不得以个人不同意为由拒绝提供产品或者服务。

个人信息处理活动中个人权利

与民法典的有关规定相衔接，草案对个人信息处理活动中个人的各项权利进行了明确，包括**知情权、决定权、查询权、更正权、撤销权、删除权**等，并要求个人信息处理者**建立个人行使权利的申请受理和处理机制**。

对个人信息处理者要求

草案“个人信息处理者”界定为“自主决定处理目的、处理方式等个人信息处理事项的组织、个人。”

草案明确了个人信息处理者的合规管理和保障个人信息安全等义务，要求其按照规定制定内部管理制度和操作规程，采取相应的安全技术措施，并指定负责人对其个人信息处理活动进行监督；定期对其个人信息活动进行合规审计；对处理敏感个人信息、向境外提供个人信息等高风险处理活动，事前进行风险评估；履行个人信息泄露通知和补救义务等。

对境外个人信息处理者的规定

草案规定“境外个人信息处理者”应在境内设立专门机构或者指定代表，专门负责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。

草案尚未明确机构或代表的具体要求或需要承担的法律责任。

草案还规定，境外组织、个人损害中国公民个人信息权益或中国国家安全的，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。

规定敏感个人信息范围

草案设专节对处理敏感个人信息作出严格限制。根据草案，敏感个人信息包括种族、民族、宗教信仰、个人生物特征、医疗健康、金融账户、个人行踪等。

敏感个人信息处理规定

草案设专节明确规定，基于个人同意处理敏感个人信息的，个人信息处理者**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。

草案指出，个人信息处理者具有特定的目的和充分的必要性，方可处理敏感个人信息。

草案还明确，应当向个人告知处理敏感个人信息的必要性以及对个人的影响。

处理公开的个人信息要求

草案规定，个人信息处理者处理已公开的个人信息，**应当符合**该个人信息被公开时的用途；超出与该用途相关的合理范围的，应当依照本法规定向个人告知并取得其同意。

个人信息被公开时的用途不明确的，个人信息处理者应当合理、谨慎地处理已公开的个人信息；利用已公开的个人信息从事对个人有重大影响的活动，应当依照本法规定向个人告知并取得其同意。

个人信息的“委托处理关系”的规定

草案尽管不存在“控制者与处理者”的区分，但仍然**对个人信息的“委托处理关系”做出了专门的规定，主要包括**：委托方应当与受托方约定委托处理的目的、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，并对受托方的个人信息处理活动进行监督；受托方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，并应当在合同履行完毕或者委托关系解除后，将个人信息返还个人信息处理者或者予以删除；未经个人信息处理者同意，受托方不得转委托他人处理个人信息。

公共场所收集个人身份特征信息的不得随意公开

草案规定，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。所收集的个人图像、个人身份特征信息只能用于维护公共安全的目的，不得公开或者向他人提供。取得个人单独同意或者法律行政法规另有规定的除外。

突发公共卫生事件中要严格保护个人信息

草案将应对突发公共卫生事件，或者紧急情况下保护自然人的生命健康，作为处理个人信息的合法情形之一。并明确，在上述情形下处理个人信息，也必须严格遵守本法规定的处理规则，履行个人信息保护义务。

对大数据杀熟、精准推送等自动化决策规定

自动化决策，是指利用个人信息对个人的行为习惯、兴趣爱好或者经济、健康、信用状况等，通过计算机程序自动分析、评估并进行决策的活动。

草案规定，通过自动化决策方式进行商业营销、信息推送，应当同时提供不针对其个人特征的选项，应当同时提取得个人单独同意或者法律、行政法规另有规定的除外。

草案还明确，个人认为自动化决策对其权益造成重大影响的，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。

对删除个人信息的规定

草案规定，以下情形下，个人信息处理者应当主动或者根据个人请求主动删除个人信息。

(一)约定的保存期限已届满或者处理目的已实现；

(二)个人信息处理者停止提供产品或者服务；

(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，个人信息处理者应该停止处理个人信息。

赋予必要域外适用效力

草案规定，以向境内自然人提供产品或者服务为目的，或者为分析、评估境内自然人的行为等发生在我国境外的个人信息处理活动，也适用本法；并要求境外的个人信息处理者在境内设立专门机构或者指定代表，负责个人信息保护相关事务。

个人信息保护各领域部门的职责分工

草案根据个人信息保护工作实际，明确国家网信部门负责个人信息保护工作的统筹协调，发挥其统筹协调作用。

草案同时规定，国家网信部门和国务院有关部门在各自职责范围内负责个人信息保护和监督管理工作。

相关职能部门履行的保护职责及采取的措施

履行的职责包括：（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）调查、处理违法个人信息处理活动；（四）法律、行政法规规定的其他职责。

采取的措施：（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；对有证据证明是违法个人信息处理活动的设备、物品，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。

国家机关处理个人信息的规定

草案设专节规定国家机关处理个人信息的规则，在保障国家机关依法履行职责的同时，要求国家机关处理个人信息应当依照法律、行政法规规定的权限和程序进行。

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。国家机关不得公开或者向他人提供其处理的个人信息，法律、行政法规另有规定或者取得个人同意的除外。

草案还将应对突发公共卫生事件，或者紧急情况下保护自然人的生命健康，作为处理个人信息的合法情形之一，并强调，在上述情形下处理个人信息，也必须履行个人信息保护义务。

完善个人信息跨境提供规则维护国家安全

草案明确，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处理者，确需向境外提供个人信息的，应当通过国家网信部门组织的安全评估；对于其他需要跨境提供个人信息的，规定了经专业机构认证等途径。

同时，草案对跨境提供个人信息的“告知同意”作出更严格的要求。对因国际司法协助或者行政执法协助，需要向境外提供个人信息的，要求依法申请有关主管部门批准。

对从事损害我国公民个人信息权益等活动的境外组织、个人，以及在个人信息保护方面对我国采取不合理措施的国家和地区，草案规定了可以采取的相应措施。

草案对违法行为的处罚及民事赔偿规定

草案规定，违反本法规定处理个人信息，或者处理个人信息未按照规定采取必要的安全保护措施的，由履行个人信息保护职责的部门责令改正，没收违法所得，给予警告；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。

草案同时规定，有前款规定的违法行为，情节严重的，由履行个人信息保护职责的部门责令改正，没收违法所得，并处五千万元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、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。

根据草案，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。

此外，草案还规定，对侵害个人信息权益的民事赔偿，按照个人所受损失或者个人信息处理者所获利益确定数额，上述数额无法确定的，由人民法院根据实际情况确定赔偿数额。

简述我国个人信息保护的立法进程

立法上，《中华人民共和国宪法》虽然规定了公民的人格尊严不受侵犯，公民的通信自由和通信秘密受法律保护，但民事法律长期未确立隐私权的概念。

1988 年最高人民法院在《关于贯彻执行〈中华人民共和国民法通则〉若干问题的意见（试行）》中，采取变通的方法，对隐私权以名誉权的保护方式进行间接保护，规定对侵害他人隐私权，造成名誉权损害的，认定为侵害名誉权，追究民事责任。

2003 年，国务院信息化办公室开始部署个人信息保护法立法研究工作

2009 年《中华人民共和国刑法修正案（七）》增加了“出售、非法提供公民个人信息罪”和“非法获取公民个人信息罪”。

2009 年《中华人民共和国侵权责任法》第一次在法律层面上将隐私权确定为一项独立的民事权利。

2012 年，全国人大常委会出台《关于加强网络信息保护的决定》，保护网络信息安全，保障公民、法人和其他组织的合法权益，维护国家安全和社会公共利益。

2014 年新版《消费者权益保护法》新增“第 29 条”，对经营者收集、使用消费者个人信息作出规定。

2015 年《中华人民共和国刑法修正案（九）》将“出售、非法提供公民个人信息罪”和“非法获取公民个人信息罪”整合为“侵犯公民个人信息罪”

2016 年出台的《中华人民共和国网络安全法》对个人信息安全作了原则性规定。

2017 年决通过的《中华人民共和国民法总则》，新增个人信息权。

2019 年实施《电子商务法》规定电子商务经营者保护个人信息安全的责任与义务。

2020 年出台的《中华人民共和国民法典》在第四编第六章用 8 个条文专门对“隐私权和个人信息保护”作出较为详细的规定。

2020 年，《中华人民共和国数据安全法（草案）》公开征求意见，草案明确开展数据活动的组织、个人的数据安全保护义务，落实数据安全保护责任。

综合自：《中华人民共和国个人信息保护法(草案)》及新华社、法制日报、央广网、新华网、中国信用网、民主与法制网等相关报道

评论分析

个人信息保护法将重点关注哪些方面呢?

全国人大常委会法工委发言人、研究室主任臧铁伟介绍，制定个人信息保护法——

将进一步明确个人信息处理活动应遵循的原则；

完善个人信息处理规则；

保障个人在个人信息处理活动中的各项权利；

强化个人信息处理者的义务；

明确个人信息保护的监管职责，并设置严格的法律责任。

内容来源：新闻联播　2020-10-12

个人信息保护法草案值得关注的三大亮点

一是注重敏感个人信息处理规则与金融交易中的个人信息保护

对于金融交易中的个人信息安全问题，草案给予特别关注，建立敏感个人信息处理规则就是直指在线金融交易规范。草案对敏感个人信息作出界定，并设专节明确敏感个人信息处理规则，即基于个人同意处理敏感个人信息的，个人信息处理者应当取得个人单独同意，**确保不能让“智慧支付”变成“只会支付”。**

二是注重提升技术手段，明确主体责任，依法依规信息管理

对于个人身份等基础信息，草案设专节规定国家机关处理个人信息的规则，在保障国家机关依法履行职责的同时，要求国家机关处理个人信息应当依照法律、行政法规规定的权限和程序进行。

草案特别规定国家网信部门负责个人信息保护工作的统筹协调，其和国务院有关部门在各自职责范围内负责个人信息保护和监督管理工作，建立更加高效的“一站式”监管体制，明确各个责任部门的法定职责，建立有效的投诉处理机制，真正保障个人信息保护法律制度的有效运行。

三是注重遵循“告知—同意”规则，让 App“霸王协议”成绝响

草案确立以“告知—同意”为核心的个人信息处理一系列规则，即处理个人信息应当在事先充分告知的前提下取得个人同意，并且个人有权撤回同意；重要

事项发生变更的应当重新取得个人同意；不得以个人不同意为由拒绝提供产品或者服务。（摘自：个人信息保护法能否终结“信息裸奔”）

来源：光明日报　2020-10-19

我们需要一部什么样的个人信息保护法

应当充分考虑法律可行性

陈斯喜委员认为，草案目前一些概念还比较模糊，含义不清楚，会给实施带来困难。而想**让个人信息保护法具有可行性，关键要处理好几个关系**。首先，要区分清楚公开信息收集与专门采集信息。其次，公开信息与非公开信息怎么保护要有区别。最后，要区分采集的信息是自用还是出售、转让。此外，临时采集识别与长期保存个人信息也应区分开来。比如现在一些单位、社区已经实行人脸识别，这种采集是暂时的还是永久储存的，就要区别对待。

个人信息保护立法要注意三个平衡

王超英委员认为，个人信息保护立法必须要平衡好三个问题。

一是要借鉴国际经验，更要立足中国国情。我国个人信息保护立法要考虑到我国不同于发达国家的发展水平和社会文化背景，要保证立法能够落地实施。

二是平衡好个人信息保护与数字经济发展的关系。立法既要充分保护数据主体的合法利益，也要充分重视数字经济时代相关信息和数据的合法利用问题。

三是平衡好保护个人信息和维护公共安全的关系。

数据保护法律应形成有机整体

对于个人信息保护法的法律定位，尹中卿委员认为，这是一部在民法基础上的行政管理法。因此，应在民法典基础上对自然人的个人信息隐私、对公民的个人信息权益进行保护。

对于篇章结构，尹中卿认为应当在第一章之后首先规定个人信息权益。此外，草案第二章和第三章内容目前有交叉，建议对结构进行修改予以解决。

草案问题意识还需进一步提升

全国人大宪法和法律委员会副主任委员周光权认为，制定个人信息保护法，不是说单纯地在法律的种类中增加一部法律，而是要解决目前面临的难题。此外，周光权认为，还必须考虑国家机关在取得个人信息后的管理和使用问题。同时，周光权还强调要平衡好各种关系。

来源：法治日报　2020-10-20

制定《个人信息保护法》，设置严格的法律责任

在信息化时代，个人信息保护已成为广大人民群众最关心、最直接、最现实的利益问题之一。在日常生活中，我们的个人信息随时随地都被他人获取。互联时代，不向外界提供我们的个人信息简直已经寸步难行。一些网络运营者出于自身业务拓展需要或者在客户端口预设陷阱，或者通过霸王条款强行获取个人信息，更有某些掌握他人信息的单位和人员，为了一己私利贩卖客户信息。

面对数字经济突飞猛进的发展，个人信息的商业价值也越来越大，如何解决个人信息有序获取、合理使用的问题已成当务之急。为此，有关方面曾先后出台《互联网个人信息保护指南》、《个人信息安全标准》等规范性文件，并在《民法典》、《刑法修正案九》当中明确了保护个人信息的鲜明导向，以及刑责标准。

对处理个人信息时应当遵循的诸如：目的明确、最少够用、公开告知、个人同意、质量保证、安全保障、诚信履行和责任明确等基本原则，以及信息收集、加工、转移、删除等环节有了清晰具体的认识。在总结网络安全法等法律、法规、标准的实施经验，并充分借鉴有关国际组织和国家、地区的个人信息保护相关准则、指导原则和法规的基础上，尽快建立健全适应我国个人信息保护需要的专门法律制度已经水到渠成。

制定《个人信息保护法》，将进一步明确个人信息处理活动应遵循的原则，完善个人信息处理规则，保障个人在个人信息处理活动中的各项权利，强化个人信息处理者的义务，明确个人信息保护的监管职责，并设置严格的法律责任。《个人信息保护法》实施后，我国还应参照其他国家经验设立专门的个人信息保护机构，该机构应拥有相对独立的监管、执法权力，以此全面完善我国个人信息事前保护、事后救济机制，推动个人信息保护再上新台阶。

来源：北京青年报　2020-10-14

国际变局下，个人信息保护立法的 5 大迫切性

数据同传统的物与知识产权标的有极大的区别。传统法律无法完全适用于个人数据的保护和流通。随着数字经济时代个人数据的重要价值日益凸显，亟须建立新的数据规则，在保障个人数据安全的同时促进经济发展。

加强个人信息保护是世界趋势

由于个人信息涉及个人利益、社会公共利益和国家安全，各国纷纷出台立法对个人信息进行保护。目前全球已有近 100 个国家和地区制定了有关个人信息保护的法律，发达国家基本都制定了个人信息或个人数据保护法。个人信息保护专项立法已成为国际社会共同的选择。

出台个人信息保护法的迫切性

第一，行政保护是对个人信息最有效的保护手段。

一方面，刑法主要打击严重侵犯个人信息的犯罪行为，立案标准严，保护门槛高。另一方面，民事权利的自力救济面临着取证难、找被告难、维权成本高等难题，大大限制了当事人通过民事诉讼手段寻求维权和救济。

第二，完善的个人信息保护制度有利于增强网络信任。

目前大量的数据是混合数据，包括个人信息和非个人信息。个人信息涉及公民个人的隐私安全和人身财产安全。在个人信息未得到充分保护情况下，人对网络的信任度会下降。没有完善的法律保障，就难以建立起高度的信任机制。

第三，完善的个人信息保护制度有利于数据开发、利用与共享。

个人信息保护制度不健全，数据权属不清，直接妨碍了数据在不同主体间的流通和共享，从而限制了对数据的进一步开发和利用。

第四，完善的个人信息保护制度有助于企业参与国际竞争。

个人信息保护成为国际贸易壁垒和地缘政治博弈的工具。

完善的个人信息保护立法在一定程度上有助于树立良好的保护隐私和个人信息的国际形象，为我国企业“走出去”参与国际竞争提供良好的制度环境。

第五，完善的个人信息保护立法有助于我国参与国际规则的制定。

在经济全球化、网络化、数字化的背景下，数字贸易快速增长，各国竞相出台本国的数据政策与法律，由此带来的冲突也与日俱增。

来源：网络传播杂志　2020-10-16

全国政协委员殷兴山建议加快个人信息保护专项立法进程

四点建议——

（一）加快立法进程

通过专门立法，统一对公私领域的个人信息保护，明确运营主体收集、使用个人信息的原则、程序和保密、保护义务，不当使用、保护不力的法律责任以及监管部门的监督手段和处罚措施等。

（二）设立专门监管机构

建议在立法中明确专门机构负责或牵头负责个人信息保护工作，建立统一的制度规范，有权监督运营主体，并对违规行为进行处理。若采取牵头负责模式，监管机构要发挥协调职能，相关部门应依法配合。

（三）确立运营主体运营规范

一是明确运营主体必须依法采集、使用、保管个人信息，有明确正当的目的，符合“最少、必需”要求，并经过信息主体明示同意。

二是注重平衡保护，在强调个人信息保密义务的同时，明确基于法律规定、社会公共利益、当事信息主体同意等例外规定，实现特定情形下个人信息无障碍流通。

三是加强从业人员管理，制定信息收集、处理、传输、公开、使用规则，做好流程监控，一旦发生信息泄露事件，严格追究相关人员责任。同时将技术防护纳入法律规范，推动运营主体加大技防投入。

（四）赋予信息主体自我保护权力

一是明确“信息自决权”，信息主体有权决定是否告知或允许他人利用自己的信息。建立“知情同意”制度，只有信息主体知情同意，运营主体方可采集、保管、使用个人信息。

二是赋予“被遗忘权”，借鉴欧盟《通用数据保护条例》，信息主体行使“被遗忘权”时，运营主体不仅要删除自己所掌握的信息，还要对公开传播的信息负责，有义务通知其他人停止利用并删除。

三是赋予审查、拒绝权。信息主体有权审查运营主体的适格性，仅向合法运营主体提供个人信息，对超范围收集信息，有权提出异议或拒绝提供。

四是赋予救济权。当信息主体发现信息被滥用或泄露，有依法寻求行政、民事乃至刑事救济的权利。（摘自：「两会时间」全国政协委员、人行杭州中支殷兴山：我国尚无个人信息保护专项立法建议加快进程）

来源：经济观察报　2020-05-21

相关法规

《网络安全法》与个人信息保护

法案六大突出亮点

一是明确了网络空间主权的原则；二是明确了网络产品和服务提供者的安全义务；三是明确了网络运营者的安全义务；四是进一步完善了个人信息保护规则；五是建立了关键信息基础设施安全保护制度；六是确立了关键信息基础设施重要数据跨境传输的规则。

重点解决个人信息保护的痛点问题

(一)规范了相关网络安全监管部门的责权范围

《网络安全法》规定，中央网信办为国家层面上的网络安全协调机构，公安部、工信部等涉网部门职责分明，有助于推动相关部门共同保障个人信息安全。

(二)明确了个人信息保护相关主体的法律责任

《网络安全法》进一步规范了网络运营商、关键信息基础设施运营者、网络产品、服务的提供者等相关信息采集主体必须履行的法律责任，明确了个人信息的使用权边界，有助于从源头上遏制非法使用个人信息的行为。

(三)提高了个人对隐私信息的管控程度

《网络安全法》通过引入了删除权和更正制度，进一步提高了个人对隐私信息的管控程度。

(四)增强了针对侵犯个人信息权益行为的威慑

一方面，《网络安全法》明确了对侵害公民个人信息行为的惩处措施。另一方面，《网络安全法》客观上增加了相关运营单位发生信息安全事件的成本。（摘自：①《网络安全法》筑牢个人信息保护的法律防线.理论网　2016-11-21；②《网络安全法》今起实施个人信息保护进一步完善.民政部信息中心　2017-08-28）

网络安全法中有关个人信息的部分内容

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。

……

——来自《网络安全法》

《民法典》时代，个人信息如何保护?

第一，明确了自然人对其个人信息的权益属于民事权益。处理自然人个人信息的主体无论是国家机关还是非国家机关（如企事业单位），也无论其处理的目的是行政管理、公共服务还是营利，处理者与自然人之间都属于平等的民事主体。它们之间的权利义务关系属于民事权利义务关系，自然人对其个人信息享有的属于民事权益，而非公法上的权利。这对于后续制定个人信息保护法中解决政府数据处理活动的制度设计具有重要意义。

第二，明确了自然人的个人信息权益属于人格权益。民法典虽然没有明确规定个人信息权的概念，但其明确了自然人的个人信息权益在性质上属于人格权益，而非财产权益，明确地规定个人信息权益属性的法理依据是对个人信息保护的重大进步。

第三，重新定义了隐私权与个人信息保护制度的关系。民法典人格权编将隐私权与个人信息保护合并规定在一起，同时还明确了个人信息中私密信息适用隐私权和个人信息保护的规定。这表明了我国法律明确区分了隐私权与个人信息，它们不是互相取代的关系，而是既有区别又密切联系的两种制度。

第四，明确了处理个人信息的原则、条件以及免责事由。民法典对于处理个人信息的原则、条件、免责事由的规定使得产业发展与权益保护取得了一定的平衡，

留下了更多的弹性空间。个人信息行为规制模式的规定有效弥补了个人信息人格权益的弱支配程度，同时这种侧重于事后的行为规制模式也对数据企业使用个人信息画出了红线，为信息产业的发展提供了诸多可能性。

第五，阐明了自然人、数据收集者与控制者、国家机关及其工作人员的权利义务分配边界。自然人具有查阅、抄录、复制、请求更正、删除个人信息的权利；数据收集者、控制者必须履行保护数据安全的义务；国家机关及其工作人员必须履行对个人隐私和个人信息的保密义务。

来源：民主与法制周刊　2020-07-09

从电子商务法看个人信息保护

第二十三条，该法明确指出，“电子商务经营者收集、使用其用户的个人信息，应当遵守法律、行政法规有关个人信息保护的规定”，明确了该法对于个人信息保护遵循的指导原则。

第二十四条进一步指出，“电子商务经营者应当明示用户信息查询、更正、删除以及用户注销的方式、程序，不得对用户信息查询、更正、删除以及用户注销设置不合理条件。电子商务经营者收到用户信息查询或者更正、删除的申请的，应当在核实身份后及时提供查询或者更正、删除用户信息。用户注销的，电子商务经营者应当立即删除该用户的信息”，对用户自身信息的知情权、被遗忘权等进行保护。

第二十五条还考虑到，“有关主管部门依照法律、行政法规的规定要求电子商务经营者提供有关电子商务数据信息的，电子商务经营者应当提供。有关主管部门应当采取必要措施保护电子商务经营者提供的数据信息安全，并对其中的个人信息、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”，既阐明了电子商务经营者配合有关部门开展调查的义务，又明确了相关部门负有保护数据信息安全的责任。

来源：保密工作　2018 年 11 期

《儿童个人信息网络保护规定》亮点解读

一是针对儿童个人信息的全生命周期提出更为严格审慎的规范原则，并落实在具体规则中。明确儿童个人信息的收集、存储、使用、转移行为应当遵循正当必要、知情同意、目的明确、安全保障、依法利用的原则。

二是进一步明确儿童及其监护人针对儿童个人信息享有的各项权能。包括在收集、使用、转移、披露环节，儿童监护人的知情权、同意权，及上述环节中相关要素发生实质性变更时的再次授权；儿童及其监护人发现儿童个人信息存在误差时的信息更正权；以及发现网络运营者违法、违规收集、存储、使用、转移、披露，或撤回同意、停止服务时的信息删除权。

三是明确网络运营者针对儿童个人信息的专门性、特设性保护义务。包括专条专员、知情同意、最小存储、最小访问、泄露及停业通知、安全存储、共享、披露限制。如，专条专员——设置专门的儿童个人信息保护规则和用户协议，指定专员负责儿童个人信息保护。

四是自动例外。即通过计算机信息系统自动留存处理信息且无法识别所留存处理的信息属于儿童个人信息的，不需按照本规定操作。

来源：中国网信网　2019-09-05

《信息安全技术个人信息安全规范》2020 版

国家市场监督管理总局、国家标准化管理委员会正式发布国家标准《信息安全技术个人信息安全规范》于 2020 年 10 月 1 日实施。

与 2017 版相比，此次变化主要三方面：

一、增加了“多项业务功能的自主选择”、**“**用户画像的使用限制”、“个性化展示的使用”、“基于不同业务目所收集个人信息的汇聚融合”、“第三方接入管理”、“个人信息安全工程”、“个人信息处理活动记录”等内容。

如何获得用户同意？《规范》建议，应通过如弹窗、文字说明、填写框、提示条、提示音等形式进行提示，并且要让用户主动做出肯定性的动作，比如勾选、点击“同意”或“下一步”。

扩展的业务功能，应允许个人信息主体逐项选择同意。用户不同意的，个人信息控制者不得反复征求用户同意，除非用户主动选择开启扩展功能，且不应拒绝提供基本业务功能或降低基本业务功能的服务质量。

《规范》还要求，App 在提供业务功能的过程中使用**个性化展示**的，应显著**区分个性化展示的内容和非个性化展示的内容**，比如标明“定推”字样。同时，App 应提供不针对用户特征的选项。

二、修改了“征得授权同意的例外”、“个人信息主体注销账户”、“明确责任部门与人员”、附录 C、“实现个人信息主体自主意愿的方法”等内容。

规范明确，隐私政策的主要功能为公开个人信息控制者收集、使用个人信息范围和规则，不应将其视为根据个人信息主体要求签订和履行的合同。

三、针对个人生物识别信息方面的要求，进行细化并完善。

规范规定在收集个人生物识别信息前，应单独向个人信息主体告知收集、使用个人生物识别信息的目的、方式和范围，以及存储时间等规则，并征得个人信息主体的明示同意。

规范对生物识别信息的存储提出了具体的解决措施。

第一，个人生物识别信息要与个人身份信息分开存储；

第二，原则上不应存储原始个人生物识别信息，可采取的措施包括但不限于：仅存储个人生物信息的摘要信息；在采集终端中直接使用个人生物识别信息实现身份识别、认证等功能；在使用面部识别特征、指纹、掌纹、虹膜等实现识别身份、认证等功能后删除可提取个人生物识别信息的原始图像。

来源：雷锋网　2020-03-08

《数据安全法(草案)》涉及个人信息保护的部分条款

……

第八条开展数据活动，必须遵守法律、行政法规，尊重社会公德和伦理，遵守商业道德，诚实守信，履行数据安全保护义务，承担社会责任，不得危害国家安全、公共利益，不得损害公民、组织的合法权益。

……

第二十九条任何组织、个人收集数据，必须采取合法、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，不得超过必要的限度。

……

第三十三条境外执法机构要求调取存储于中华人民共和国境内的数据的，有关组织、个人应当向有关主管机关报告，获得批准后方可提供。中华人民共和国缔结或者参加的国际条约、协定对外国执法机构调取境内数据有规定的，依照其规定。

……

——《数据安全法(草案)》

国外怎么保护个人信息?

美国采用分散立法和行业自律相结合的模式保护个人信息。

1890 年路易斯·布兰代斯和塞缪尔·沃伦发表的《隐私权》一文中，把隐私定义为“免受外界干扰的、独处的”权利，隐私权成为一个正式的法律概念并对美国立法产生了巨大影响。二十世纪六七十年代后，美国隐私权不断向立法领域扩张。但美国并没有形成一部保护个人信息的隐私权的综合性法典，对个人信息的隐私权的保护仍散见于联邦和州政府制定的各类隐私和安全条例中，如在儿童信息、医疗健康、金融数据等敏感领域，制定了《儿童在线隐私权保护法案》《健康保险携带和责任法》《金融服务现代化法案》等法律保护个人信息安全。

除了分散立法保护个人信息之外，美国还采取行业自律的方式对个人信息提供保护，以满足立法滞后于现实的需要，目前美国的行业自律形式有建议性的行业指引、网络隐私认证、技术保护模式这三类。

德国采用统一立法的模式保护个人信息。

德国从“人格尊严”的视角来看待公民个人信息法律保护问题，将公民个人信息划归于人格权的基本权利范畴之中。德国联邦法院通过人口普查第一案和第二案，在实践中确认了公民个人信息的宪法权利地位。1970 年德国黑森州颁布了《黑森州资料保护法》，这是一部关于公民个人信息法律保护的专门立法，但是这部法律没有确立独立的个人信息权，直到 1978 年生效的《联邦数据保护法》，才正式赋予个人一般性的个人信息权利。同时，该法对侵犯公民个人信息的违法犯罪行为进行了详细说明，并明确了对相关违法行为的处罚形式。统一立法模式通过国家在公私领域对公民个人信息进行统一保护，可以使公民个人信息权利成为一项具有绝对性的法律权利，同时有助于统一标准，又可以避免行业自律模式各行其是的弊端，更能助推公民权利的实现。

日本采用统一立法和行业自控相结合的模式保护个人信息。

日本政府对个人信息的保护始于日本推进政府办公电子化。2005 年正式实施的《个人信息保护法》是日本保护个人信息安全的基本法，该法的主要目的是个人信息的有效利用和保护。日本在制定个人信息保护法律法规的同时，充分借

鉴美国的行业自律模式，通过行业自控来实现自我规范、自主规制。经过长期的实践，日本形成了公共部门立法规制，非公共部门实行行业自控，特殊领域个别立法的个人信息保护基本原则。日本统一立法和行业自控相结合的个人信息保护制度模式在公民个人信息保护与公民个人信息流动之间找到了平衡点，既吸收了美国“隐私权”的内核，又尊重本国行业自律自控的特性，切实保护公民的个人信息。（摘自：民法典时代，个人信息如何保护？）

来源：民主与法制周刊　2020-07-09

简要认识欧盟最严数据保护法案

欧洲议会颁布的《一般数据保护法案》（以下简称“GDPR”）于 2018 年 5 月 25 日在欧盟各国正式生效。作为一部用来保护欧盟公民个人隐私和数据安全的新法案，其颁布使得欧盟对于数据保护的监管达到了前所未有的高度。

该法案把可以直接或间接识别到的某一个个体的任何信息都视为个人信息，包括了从姓名、照片、身份证号、邮箱地址、银行账户、健康记录到网络用户名、位置定位、社交媒体发布的信息、计算机 IP 地址等各个方面，堪称目前世界范围内最宽泛的个人信息定义。作为一部用来保护欧盟公民个人隐私和数据安全的新法案，其颁布使得欧盟对于数据保护的监管达到了前所未有的高度。

GDPR 对于个人数据泄漏通知做出了明确规定。当发生个人数据泄漏事故之后，企业要在发现后 72 小时内向监管机构报告,并对报告的内容做了详细的规定。

GDPR 对于企业违规设置了昂贵的处罚规定。对于不遵守 GDPR 法案的企业处以严厉的制裁和巨额罚款，根据违规性质的严重程度，分为一般违法行为和严重违法行为。对于一般违法行为，处以全年营收额 2%或 1000 万欧元的罚款，两者以高者为限；对于严重违法行为，处以全年营收额 4%或 2000 万欧元的罚款，两者以高者为限。

GDPR 不仅适用于在欧盟国家注册的组织机构,也同样适用于任何在欧盟以外地区注册但为欧盟地区提供商品和服务,并监控个人行为和数据信息的组织机构。**对于任何持有和处理欧盟国家公民个人信息的公司无论其公司所在地，皆受该法案管辖。**（摘自：欧盟最严数据保护法案来了网络安全保险需求被推高）

来源：中国保险报网　2018-08-10

综述：欧洲以立法形式保护个人“被遗忘权”

欧盟颁布《数据保护通用条例》的第１７条**“被遗忘权”特别指出，当个人数据已和收集处理的目的无关、数据主体不希望其数据被处理或数据控制者已没有正当理由保存该数据时，数据主体可随时要求收集其数据的企业或个人删除其个人数据。**

欧盟委员会正是在这份法律文件中首次提出“被遗忘权”这一新型权利，引人注目。

欧洲法院在２０１４年的一次司法审判中做出了有利于一家西班牙数据保护机构的判决，互联网公司被要求承担消除数据的责任，这被认为是“被遗忘权”的重大胜利。正是在那次审判后，欧洲公民申请消除个人数据的处理机制得以建立。

“被遗忘权”的概念产生后，始终伴随争议。支持者认为，它是调整网络用户与网络公司悬殊力量的重要砝码，是对人权的及时扩充；反对者则坚称，这一权利带来“如何平衡数据保护与言论自由”的问题，在技术上也难以实现。

有专家指出，在欧洲立法保障“被遗忘权”的进程中，网络用户的诉求与国家安全战略紧密相连，共同制衡强大的数据控制者，将消弭网络时代数据主体和数据控制者的不平等。

来源：新华社　2017-08-11