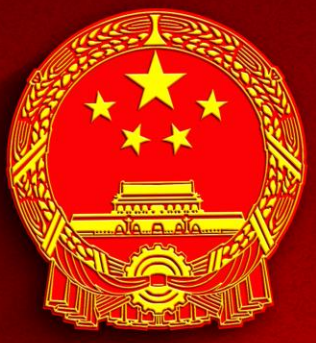


热烈庆祝 浙江省十二届人大五次会议 浙江省政协十一届五次会议 隆重召开

大数据时代的个人信息安全

—宁波市图书馆—

浙江省公共图书馆信息服务联盟

目 录

免责声明:

浙江“两会”专题信息产品由浙江省公共图书馆信息服务联盟各成员单位联合编辑。信息内容采自公开的报纸、图书、期刊、数据库资源以及各大主流网站，每份专题我们都准确标明来源和出处，摘选信息内容的真实性、准确性和合法性由发布单位负责。

本期专题由宁波市图书馆编辑，如您需要更为详细的内容及跟踪报道，请与该馆联络。

大数据时代的个人信息安全

随着互联网技术的不断普及，人们生活的各个方面都开始与网络息息相关，网上购物、网上缴费等各种活动都开始网络化，人们的信息也开始不断地暴露到各个软件之上，个人信息的安全系数不断降低。公民个人信息的安危不仅仅是公民个人人身、财产安全问题，还关系到整个社会的安全稳定。面对公民个人信息不断暴露，公民个人人身安全不断受侵犯的情况，公民的个人信息保护变得更加迫切。

大数据时代的个人信息界定

大数据时代的个人信息

目前各国及国际组织对“个人信息”的界定可分为“概括式”和“列举式”两种，无论采取何种方式界定个人信息，各国公认“识别性”构成了个人信息的一般特征。具体到我国，2012 年 12 月 28 日，全国人大常委会通过《关于加强网络信息保护的决定》，其中第 1 条明确规定“国家保护能够识别公民个人身份和涉及公民个人隐私的电子信息”。因此，个人信息是指与一个身份已经被识别或者身份可以被识别的自然人相关的任何信息，包括个人姓名、住址、出生日期、身份证号码、医疗记录、人事记录、照片等单独或与其他信息对照可以识别特定的个人的信息。

在大数据时代，信息成为一种资产，个人信息的商业价值日渐突出，与此同时也带来了对个人信息保护的挑战。个人信息的自动化处理，使原来不具有意义的信息片段具有了意义，个人信息经过自动化处理，可以提取出一些信息主体不欲人知并且未在其提供的信息中直接显示出来的隐私。例如，在网上由信息主体或他人所发布的个人碎片信息，按照既有标准是不构成隐私的，但将这些碎片进行整合分析后，得出的结果却可以勾勒出信息主体的“数据形象”，所以在此情况下，已不再有所谓不重要的资料。公共场所被拍摄的视音频资料、QQ 和微信等社交软件账号密码、社交网站的朋友动态、IP 地址及手机位置信息、上网及网购记录等传统隐私法中被排除在外的因素，在大数据时代都可能被纳入到个人信息概念的外延之中。

大数据时代个人信息的双重属性

德国学者冯·图尔说：“权利是私法的核心概念，同时也是对法律生活多样性的最后抽象。”传统民法理论中，一个客体对应一种利益或权利，但在知识产权和某些精神性人格权的形成过程中，其对象负载的利益不仅包括人格利益，也逐渐包括了财产利益。当客体所负载的利益随着社会实践的发展而不断丰富，原有制度已经容纳不下这种现象，学界应该做出积极的回应，以纠正理论与实践的偏离。

1.个人信息的人格价值维度

根据大陆法系人格权理论，凡是与人格形成与发展有关的情事都属于人格权客体。个人信息所体现的是公民的人格利益，个人信息的收集、处理或利用直接关系到信息主体的人格尊严。个人信息通过显现个人的生活轨迹，勾勒出个人人格形象，与信息主体人格密不可分。因此，个人信息对于信息主体的人格尊严和自由价值，应当是个人信息保护立法中首要考虑的因素。然而，在制度方法的选择上，采用单纯的人格权制度是否能为个人信息提供充分保护呢？个人资料体现的人格利益远远超出了具体人格利益的范围，这也是现有法律框架无法对个人资料提供切实、充分保护的根本原因。而如果个人信息同时兼有维护主体人格尊严和财产利益的价值或功能时，就应该给予其人格权和财产权的双重保护。在大数据时代，个人信息权在客体、内容、行使方式等方面有别于传统的具体人格权（ 如隐私权、肖像权），并发挥着这些权利不可替代的作用，个人信息保护法应该将其确认为一项新生的独立权利。并且，鉴于个人信息特殊属性，应该在我国法律体系内为个人信息建立区别于其他具体人格权和财产权的专门的权利制度，即“个人信息控制权”，简称“个人信息权”。

2.个人信息的财产价值维度

从 2008 年开始，大数据交易市场已初见端倪，“数据市场”、“数据银行”、数据交易市场已成为新型的经济形式。2013 年 4 月，一位名叫 Federico Zannier 的美国人在网上拍卖自己 3 个月积攒的大约 7 GB 的隐私数据，并成功炒到 1100 美元。虽然是个例，但个人信息的商品属性已经不容回避。从目前已成规模的“数据市场”和它们所创造的巨大经济价值来看，实践已经先于理论，率先明确了个人信息的财产价值。

根据经济学理论，法律上的财产必须符合三方面的条件： 一是因稀缺而具有价值； 二是能够归属于某一特定主体拥有，该主体能够排除他人的共享和干涉； 三是能够以一定价格让渡给他人。17 世纪的威尼斯国王为了能使伽利略的技术方案得到保护，用法律手段赋予他对其发明创造的排他性使用权和转让权，使技术方案具备了作为“财产”应当具备的第二个和第三个属性，一种新的财产权产生了，

那就是知识产权。以史观之，如今“在路上”的个人信息权与当初的知识产权何其相似。

在目前的时代条件下，个人信息的使用价值已被承认，而价值的实现必须通过交换，财产价值私有化则是交换的前提，所以，只有通过法律制度对个人信息财产属性的确认，才能实现个人信息的财产价值。波斯纳曾指出：“无形财产权的一个非常规的例子是隐私权（Right of Privacy），它通常被作为是侵权法的一个分支讨论，但从实际情况看，它确实是财产法的一个分支。”美国学者 Miller 也指出：也许保护隐私最容易的途径是将对个人信息的控制作为数据主体拥有的财产权，能享有宪法和法律对财产所给予的全部保护。美国另一学者 Shorr 主张将“个人数据财产化”（Propertization of Personal Data），确认个人对个人数据拥有所有权，以便用财产权模式来保护个人数据。从实践角度看，对个人信息的财产化利用已经成为大数据时代不可逆转的趋势，从理论角度而言，承认个人信息财产价值符合经济学理论，在英美法中亦具备相当坚实的法理基础。因此，在制定我国的个人信息保护法时，必须充分考虑到个人信息财产价值维度，并用确权的方式将之明确。（来源：《北京邮电大学学报》2016 年 10 期）

个人信息安全的现状

个性化定制时代的个人信息危机

今天是一个个性化定制时代。打开购物网站，淘宝告诉你这是为你私人定制，全球独一份；打开新闻网站，除了常规新闻，还有“你喜欢的新闻”的栏目，微博、微信更将这种个性化服务发挥到极致，看到的都是你关注的内容，不想看的关掉即可。

用户享受的是宾至如归的服务，权利被尊重，爱好被迎合，虚荣心得到了满足。但大部分用户并未清醒意识到的是，各个平台在打造自己的个性化服务的同时，也在贪婪地抓取个人数据，经过加工、分析后变现。

概括地说，今天所有个性化商业服务的基础，正是个人源源不断

产生的数据流。

2016 年 6 月底，谷歌把 2007 年曾向用户承诺的隐私条款不动声色地拿掉了：“除非用户同意，谷歌不会将下属广告公司 Double Click 收集的 cookie 信息，和谷歌收集的其它个人身份信息结合起来使用”。Double Click 是谷歌的广告服务平台，移除旧条款意味着，谷歌可以把用户的网上浏览记录和用户邮箱、用户搜索所留下的数据联通，建立完整的用户行为链，为其精准地推送广告服务。要强调的是，谷歌邮箱包含大量的实名信息。

也就说，网民的上网行为透明了。谷歌甚至可以通过分析用户的邮件内容，推断用户的需要并推送相应广告。

这件事正在美国发酵。谷歌发言人回应称，这是为了适应当下的“智能手机革命”。这当然是堂而皇之的“官方”解释。

这表明了商业机构对个人信息的使用，已经到了公开化、常态化、系统化阶段，数据不仅已经成为隐私最主要的载体，而且带有明显的经济属性。过去，隐私被侵犯后主要给个人带来精神上的伤害，如名誉受损；今天，数据是隐私的载体，它的经济价值被企业觊觎，更多地在经济活动中被使用，甚至可以成为个人私有财产的一部分。

事实上，即使在美国，谷歌已经是隐私保护阵营中最后的坚守者。近十年来，把互联网上收集的用户行为数据和线下的单位名录等数据进行对比、匹配，以确定每一个人的行为，几乎是每一家互联网公司甚至是实体企业都在悄悄做的事。每成功匹配一个用户数据，都给广告商带来打鸡血般的兴奋。

对于这一点，公众并非毫无察觉，但为了电子化生活的便利，为了得到商业机构的个性化服务，有越来越多的人愿意“让渡”自己的部分隐私。

让渡了哪一部分呢？为了厘清隐私被侵犯的脉络，有学者把隐私分为“门内隐私”和“门外隐私”。

“门内隐私”即一个人贴身的活动，例如性行为、亲密关系、家庭生活等。网上浏览记录、网购行为和社交媒体记录，可以认为是“门外隐私”，通过这些数据，商家可以推断你个人的消费习惯和生活习惯。很多时候，个人如果向商家“出让”自己的这部分隐私，可以换

取购物、出行、就餐、旅行等生活行为的方便。

正是借助窥视、占有“门外隐私”，网购平台会送上秀色可餐的商品，让人欲罢不能，新闻网站在一次次数据抓取分析加工中形成用户画像，顺带附上一个小广告、一篇软文。地图开发商一边在向用户提供着服务，一边收集用户数据，一边在向平台中的商家收取费用。

这种“让渡”无疑成全了商业机构，成全了它们所谓的盈利模式，让它们可以从容地变现数据的经济价值。但是，这里面存在许多问题，非常微妙，即使是门外隐私，也不代表完全安全。

2016 年 10 月，美国真人秀明星金·卡戴珊在巴黎遭遇持枪抢劫并被绑在浴室，价值 7000 万的珠宝被抢。与很多人喜欢在朋友圈分享吃喝玩乐经历一样，卡戴珊也是社交媒体的拥趸，她在推特、Instagram 上拥有数千万名粉丝。刚抵达巴黎，她就不断分享时装秀、晚宴、食物和首饰等在巴黎的点点滴滴。

案发后，安全专家分析，卡戴珊的遭遇与她在社交媒体频繁分享生活动态不无关系，这些分享透露出了她的地理位置和行踪，加上大量珠宝照片，因此被劫匪盯上。卡戴珊获救后，从此沉默，再也没有更新过自己的社交媒体。

中国方面也有类似新闻，《法制晚报》就曾报道，通过微信“附近的人”功能，连续变换 3 次以上位置，再辅以电子地图，就能定位出其他微信用户的位置，甚至有犯罪分子借助微信定位搜寻“猎物”。

《大数据》这本书中也讲过一个有趣的例子，说明貌似不相关的数据却可能泄露你致命的隐私。有银行在某地新安装了一部 ATM 机，却发现每天午夜 12 点到 2 点有大量款项被取走。银行担心诈骗，雇用侦探专门调查之后却发现：该提款机靠近一家色情俱乐部，顾客提取现金的目的，是不想在信用卡留下“不体面”的消费记录。很快，当地报纸登出一条新闻：“×× 银行知道昨晚谁光顾了妓女”。人们从 ATM 机上取钱，留下的数据虽然仅仅是一笔银行交易，但加上位置信息，可能就暴露了提款的目的。

以上案例表明，一条数据的信息量可能非常有限，但多条数据经过整合、分析、合成后，信息量可能倍增。即零散的数据可能被“合成”，它们可以相互解释、彼此印证，“门外”的最终可以变成“门

内”的，对隐私和安全产生“1+1>2”的穿透力。（来源：大参考 2016-11-28）

个人信息交易现状与隐忧

1. 个人信息交易现状

在大数据时代，数据本身即经济，数据产业已经成为新型经济形态。在这个特殊的时代，个人信息从未像今天这样被如此方便地搜集、整理、分析、利用，并焕发出巨大的价值； 个人信息也从未像今天这样，被如此轻易地传递、交易、滥用、侵犯。对个人信息而言，“这真是一个最好的时代，也是一个最坏的时代”。

目前，许多国家或国际组织都将个人信息视作重要的经济资源，并将数据产业提升为国家战略。

美国、欧盟、日本等信息服务较为发达的国家不仅通过个人信息保护的法制建设，树立本国的数据战略优势，更通过建立规范的个人信息交易市场的方式，充分发掘个人信息的商业价值。如日本富士通公司于 2013 年建立的“Data Plaza”交易市场、美国的 Personal 公司和 Reputation 公司等，都属于个人信息的交易平台，这些平台通常都以个人信息的稀缺性和财产性为基础，将个人信息资源作为一种新型资源加以配置流通，创造着巨大经济价值。利用此类平台，信息主体可以用信息换取现金回报或折扣优惠，企业也可将信息用于商品开发和打造新业务。我国政府也积极顺应大数据的时代潮流，“十三五”规划建议提出：：“实施国家大数据战略，推进数据资源开放共享。”2015 年 4 月，我国第一个大数据交易平台也在贵阳正式挂牌运营并完成了首批大数据交易。许多互联网企业如阿里、腾讯等已经在主动收集用户信息，意识到了个人信息重要价值的政府部门也开始自主收集或向企业索取个人信息。

2.繁荣之后的隐忧

与快速发展的个人信息交易相比，由于个人信息权利的法律界定一直不明朗，标准不清、监管缺失、责权不明等问题不可避免地出现在我国的个人信息交易中。有学者已经开始担忧，信息交易市场“只有买方和卖方的利益，没有元数据所有者，更没有个人隐私跟公众利益

的位置”。

（1） 个人信息滥用现象严重

我国法律并未将信息权利的主体明确为“本权”，权利主体的不明确，导致目前的个人信息市场中，个人信息的流转完全脱离本人，真正的信息主体既无法控制信息的流向，更无法实现对信息财产的收益，对个人信息的滥用日益猖獗。出于对隐私风险的惧怕，信息权利人会倾向于“最小化”地提供信息，并对信息利用产生抵触情绪，最终将影响个人信息资源的价值最大化。

（2） 个人信息保护标准缺位

我国刑法有“出售、非法提供公民个人信息罪”。意味着非法的个人信息交易会受到法律制裁，但是，经过权利人授权的合法个人信息流转又该遵循怎样的规则呢？法律却尚未给出答案。个人信息的清洗需要达到怎样的标准，又需要符合怎样的交易规则，对交易主体又有何限制？在这些问题的答案尚不明朗的情况下，海量信息就被挂牌交易，无论对个人信息主体还是市场秩序，都充满了风险。法律的回避造成了目前个人信息流转的无规则，黑市猖獗，“潜规则”横行。

（3） 正规信息分享机制缺失

在合法的信息分享机制缺位的状态下，出于对信息交易合法性的考虑，许多企业不敢到黑市购买信息，又无法从正规渠道获得个性化的信息产品，创新能力受到限制。即便到个人信息“黑市”买来了信息，企业仍然难以获得有效和精准的个人数据，因为黑市交易的个人信息一般都是“粗加工产品”，质量很差、错误百出并且很难得到更新。未得到法律认可的“信息公司”从事的是信息的简单搜集活动，缺乏对信息进行深度加工的技术水平，信息附加值不高，难以成为符合企业需求的有效的信息资源，更遑论对信息主体的匿名化处理与保护。

根据欧盟《数据保护指令》，只有在第三国提供“充分保护”时才准许个人信息的国际传输，在大数据时代，我国只有尽快建立规范的个人信息保护和流转规则，才能在国际竞争中占领战略制高点。（来源：《法制日报》2016-09-18）

个人信息安全和隐私保护报告

在对全国 100 多万份调查问卷进行系统分析研究后，《中国个人信息安全和隐私保护报告》（以下简称《报告》）于 2016 年 11 月发布。调研显示出，当前公民个人信息遭受侵害的程度，令人触目惊心。

《报告》披露：超过七成以上的人都认为个人信息泄露问题严重；多达 81%的人收到过对方知道自己姓名或单位等个人信息的陌生来电；53%的人因网页搜索、浏览后泄露个人信息，被某类广告持续骚扰；在租房、购房、购车、考试和升学等个人信息泄露后，受到营销骚扰或诈骗的高达 36%。

两成人曾受电信诈骗恐吓

由中国青年政治学院互联网法治研究中心和封面智库联合发布的这份《报告》显示，有 26%的人每天收到 2 个以上的垃圾短信，20%的人近一个月来每天收到两个以上骚扰电话。

《报告》还显示，在遭遇个人信息侵害时，经历邮箱、即时通讯、微博等网络账号密码被盗的参与调研者占 40%，因在网站留下个人电话和注册网络金融服务而遭遇各类骚扰和诈骗的参与调研者都在 30%以上，遭遇针对银行卡、信用卡和网络交易诈骗以及被“短信炮”、“拨死你”电信骚扰的参与调研者比例在 20%以上，被冒充公检法、税务机关的不法分子诈骗、恐吓的参与调研者比例达 19%，明确知道个人和家庭信息被贩卖、泄露的参与调研者比例达 18%。

此外，即便最少的数据比例，即“个人隐私信息被网站公布”、“购买机票后收到航班异常的电话或短信诈骗信息”也达 9%。

60%受访者不知如何维权

在日常生活中，证件复印件、快递单和手机是泄露个人信息的重要载体。《报告》显示：有高达 55%的人将证件复印给相关机构时，从不注明用途；47%的人经常将写有个人信息的快递单直接扔掉而不加处理；超过 27%的人在停用、注销手机号的时候，甚至不去银行、支付宝、网站等变更绑定的手机号。

在被问到发现个人信息泄露会采取什么行动的问题时，71%的参与调研者选择了掐断电话或不予理睬，选择拉黑及拒接的比例为 63%；仅有 20%左右的参与调研者选择了举报、投诉、报警等积极应对措施。

在解释未能维权的原因时，半数以上的参与调研者因不知如何维权（占 60%）和没有发现经济损失（占 56%）而选择了沉默。

值得关注的是，参与调研者中有高达 44%的比例选择了因维权程序太复杂、成本太高而放弃维权，另有 34%的人是因缺少维权证据而无奈放弃。最为消极的是“维权成功也没有好处”选项，也有 14%的选择比例。

量刑过轻震慑力有限

针对此次调查发现的问题，《报告》认为，尽管目前我国针对个人信息保护存在诸多法律规定，但基本都分散在效力层次不一的各种法律法规乃至规范性文件。因此建议，应尽快通过一部统一的个人信息保护法规，对相应法律进行系统化梳理和整合。

《报告》指出，尽管当前针对个人信息的非法获取与利用的司法判决为数不少，但与个人信息泄露的普遍状况相比，并不成比例。特别是个人信息泄露与电信诈骗等犯罪活动结合之后，造成了重大的损失和巨大的社会影响，亟需加大惩处力度，增加犯罪成本，以切实起到威慑作用。

“我们做了一个案例数据库检索，只找到相关的 40 多个案例的判决书。而在这其中，只有 5 个案例是判决侵犯个人信息的罪犯是超过一年，超过两年的更是仅有两个案例。这样的比例也说明，我们刑法的量刑规定不是很高，在实践中震慑力还比较有限。这同样也印证了维权困难导致受侵害人维权意愿低下的观点。”《报告》执笔人、中国青年政治学院互联网法治研究中心执行主任刘晓春说。

中国青年政治学院副校长、互联网法治研究中心主任，最高人民法院刑一庭副庭长林维认为，应建构统一的立法框架、加大司法打击力度、确立顺畅维权渠道。“把关注的焦点从事后的惩处转移到事前的防范上来，从非法数据产业链的源头堵住数据泄露的可能性，才有希望从根本上治愈这一顽疾，迎来个人信息保护的蓝天。”

芝麻信用成实践样本

《报告》同时指出，实现健康市场秩序的具体模式，其构架可以通过建设“基础法律规范、行业通用标准、企业最佳实践”的架构来实现。

在此方面，刘晓春介绍，经过《报告》课题组专家调查研究，建议可根据芝麻信用等征信机构形成的实践样本，提高征信机构和数据信息行业的准入门槛，建立个人信息分类保护、全面落实用户授权机制、严格规范内部管控流程、完善泄露危机应急预案，让这个成为整个数据信息行业的通用标准。

例如，以手机 app 等软件为例，芝麻信用等企业建立内部信息采集规范，只采集与评估用户信用状况有关的信息，而不采集用户的聊天、通话等个人隐私信息，不得追踪用户在社交媒体上的言论信息。

同时，芝麻信用在合作伙伴的选择上实行类似于“黑名单”制度，设立了外部舆情监测机制，一旦发现合作商户存在信息泄露或违法违规采集/输出用户信息的情况时，会及时评估事件对用户信息安全造成的风险或潜在威胁，甚至决定中止或终止与合作商户的合作。

蚂蚁金服副总裁、芝麻信用总经理胡滔在会上透露，芝麻信用已通过英国标准协会权威评估认证，成为国内首家获得 ISO27001: 2013 国际信息安全管理体系认证证书的征信机构。

“在信息安全管理方面，芝麻信用严格按照国际信息安全最佳实践要求实施，即使投入成本，改变流程，也要尽最大努力保护用户的个人信息和隐私安全，这也是我们对用户的承诺。我们也希望，芝麻信用阳光公约的相关原则和做法，能成为更多同业的共识。”她说。（来源：《法制日报》 2016-11-23）

侵犯公民个人信息犯罪 10 大典型案例

今年以来，公安机关网络安全保卫部门加大侵犯公民个人信息犯罪的打击力度，共侦破此类案件 1800 余起，抓获犯罪嫌疑人 4200 余人，查获各类公民个人信息 300 余亿条。2016 年 12 月 17 日，公安部发布了侵犯公民个人信息犯罪十大典型案例。

案例一：非法获取公司账号 售卖获利 10 万元

2016 年 6 月，北京公安机关网络安全保卫部门破获顾某非法获取计算机信息系统数据案。

经查，自 2016 年 1 月起，顾某伙同他人制作用于非法获取某公司账号的软件程序，并在互联网上大肆收购网站身份认证信息，使用软

件大量实施“撞库”行为，非法获取该公司账号约 10 万组，并通过互联网大量出售账号及扫号程序，非法获利 10 万余元。

案例二：江苏“K8 社工库”案查获个人信息 20 亿条

2016 年 3 月，江苏淮安公安机关网络安全保卫部门成功侦破一起侵犯公民个人信息案，抓获犯罪嫌疑人 8 名，捣毁国内最大的网络社工库“K8 社工库”（www.k8sec.com），查获公民个人信息 20 亿条。

案例三：贩卖学生及家长信息 35 人落网

2016 年 6 月，经过 1 年多的侦查，四川广元公安机关网络安全保卫部门侦破一起侵犯公民个人信息犯罪案，抓获犯罪嫌疑人 35 名，查获四川全省学生信息及家长的公民个人信息 1200 万条，打掉非法买卖学生信息牟利的犯罪利益链条 6 个。

案例四：福建“浮云网”侵犯公民个人信息案

2016 年 8 月，福建泉州公安机关网络安全保卫部门破获“浮云网”侵犯公民个人信息案，抓获犯罪嫌疑人 51 人，成功打掉买卖公民个人信息的网站“浮云网”，查获公民个人信息 2200 万余条。

案例五：山东侵犯公民个人信息案

2016 年 6 月，山东淄博公安机关网络安全保卫部门破获一起侵犯公民个人信息案，抓获犯罪嫌疑人 6 名，打掉侵犯公民个人信息的犯罪源头 2 个，查扣公民个人信息近亿条。

案例六：员工倒卖快递信息获利 30 余万元

2016 年 6 月，江苏徐州公安机关网络安全保卫部门破获一起非法获取计算机信息系统数据案，抓获犯罪嫌疑人 8 名，摧毁一条以黑客和快递公司内部员工为泄露源头的倒卖快递信息的黑色产业链，查扣各类快递信息 500 余万条，犯罪嫌疑人非法获利 30 余万元。

案例七：出售股民信息非法获利 280 万元

2016 年 5 月，湖北宜昌公安机关网络安全保卫部门破获余某某侵犯公民个人信息案，抓获犯罪嫌疑人 10 名。经查，该团伙自 2015 年 9 月至 2016 年 5 月，非法获取并出售股民信息、银行理财信息等各类公民个人信息 1100 余万条，非法获利 280 余万元。

案例八：出售公民银行信息获利 40 余万元

2016 年 6 月，山东威海公安机关网络安全保卫部门破获董某某侵

犯公民个人信息案，抓获犯罪嫌疑人 5 名。经查，2 名银行工作人员利用职务之便，非法查询公民个人银行账户余额、流水等信息进行出售，非法牟利 40 余万元。

案例九：利用“快递单号生成器”等软件牟利 3 万

2016 年 6 月，内蒙古赤峰公安机关网络安全保卫部门破获李某某侵犯公民个人信息案。经查，该团伙利用“快递单号生成器”等软件筛选快递单号，通过快递公司内部人员查询对应的公民个人信息 7 万余条，非法获利 3 万余元。

案例十：网上搜集公民个人信息出售敛财 10 万

2016 年 5 月，湖南怀化公安机关网络安全保卫部门破获一起侵犯公民个人信息案，抓获犯罪嫌疑人 5 名。经查，该团伙通过在网上购买、搜索、下载等方式大量搜集公民个人信息，再通过“撞库”“扫存”等非法软件比对公民网络账户密码，进行出售和“刷单”赢利，非法获利 10 余万元。（来源：新华社 2016-12-17）

个人信息安全的立法保护

侵犯公民个人信息犯罪的实证研究

近年来，因为个人信息泄露而引起的电话骚扰、垃圾信息、网络买卖公民个人信息高发，不仅严重干扰了人们的正常生活而且由此引发的电信诈骗、敲诈勒索、故意伤害、网络诈骗、绑架和非法讨债等犯罪案件持续高发及产生一系列连锁反应，导致公民的人身和财产安全遭到严重威胁和损失，严重危害了社会安全，使我们愈来愈重视个人信息保护的重要价值和实践意义。

1.我国侵犯公民个人信息犯罪实证统计

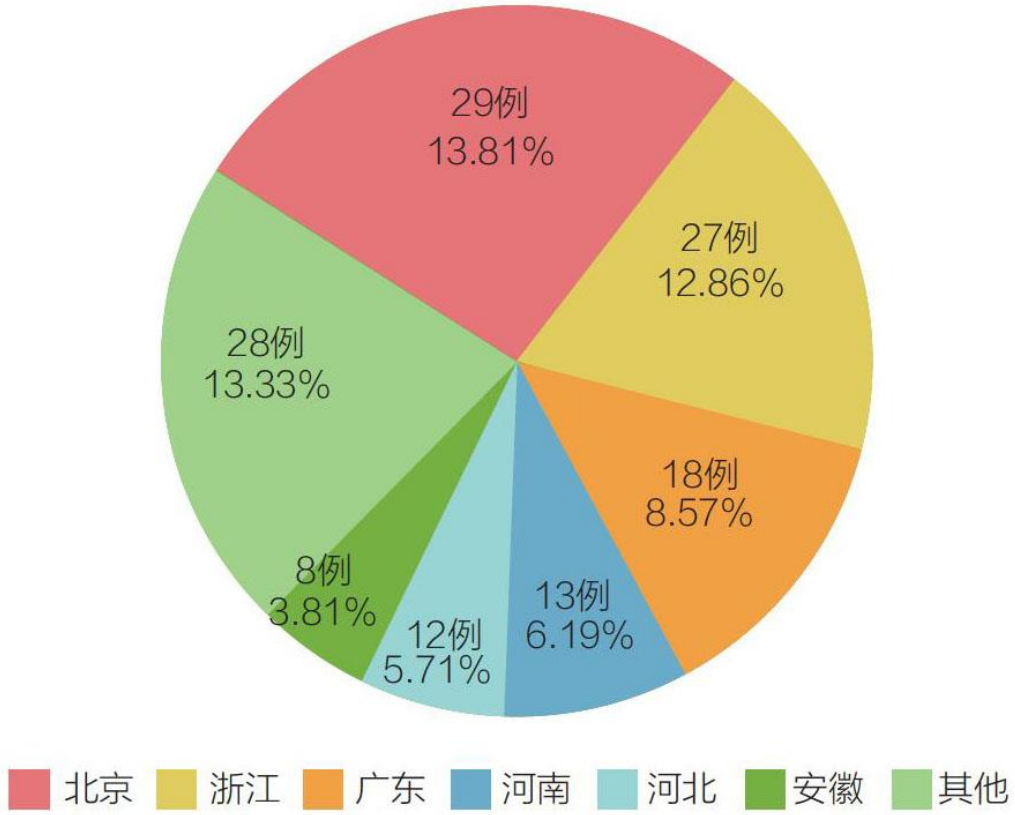
案例均来自“北大法宝”数据库。笔者在网页一栏中输入“个人信息”作为关键词搜索，检索到 2009 年 1 月 1 日至 2014 年 12 月 31 日的相关刑事案例 210 起，其中上海市案例 75 件，非上海市案例 135 件。

上海市以外各省份的个人信息犯罪情况

表一：样本总数及上海市案例占比（单位：件）

	案例总数	上海市案例	上海市案例所占比例	非上海市案例	其他省案例所占比例
案例数及比例	210	75	35.71%	135	64.29%

上海市以外各省份的个人信息犯罪情况



上述统计中，上海市出售、非法提供和非法获取公民个人信息犯罪的数量占全国总数的比例为 35.71%。在剩余的案例中，北京、浙江、广东、河南、河北、安徽等省份发生的个人信息犯罪占了全国总数的 64.29%。在这些地区的案例中，以北京（29 件）、深圳（5 件）等经济发达城市为主。从全国范围来看，天津、重庆、辽宁、甘肃等省份侵害公民个人信息案件发生频率比较低。

从样本案件逐年统计表和案件数量变化示意图可以看到，自 2009 年广东省出现第一例侵犯个人信息犯罪案件开始，特别是从 2011 年

以来案件的数量呈现逐年快速上升的态势，每年几乎上升 20 件。侵犯个人信息案件的案发省市的范围也是逐年扩大，尤其是经济发达地区案件数量增长较快，侵犯个人信息犯罪的危害也越来越严重。

从表格二可以看出在侵犯个人信息犯罪具有代表性的 182 起案件中，出售、非法提供个人信息的案件为 14 件，所占的比例为 7.7%，非法获取个人信息的案件为 163 件，所占的比例为 89.6%，两个罪名均触犯的案件为 5 件，所占的比例为 2.7%。非法获取个人信息的案件比例占所有侵犯个人信息犯罪的 89.6%，将近九成，构成了司法实践中侵犯个人信息犯罪的典型代表。

从上述表格统计可以看出，在具有代表性的 182 起案件中，因侵犯公民个人信息犯罪被判处有期徒刑缓刑的案件是 73 件，所占的比例为 40%；单处罚金的案件为 11 件，所占的比例是 6%；一年以下有期徒刑（含拘役）的案件是 142 件，所占的比例为 78%；1 年到 3 年有期徒刑的案件是 29 件，所占的比例为 16%。和其他侵犯公民人身财产权益案件相比，公民个人信息犯罪被判处刑罚整体较轻，这在笔者对司法机关进行实地走访时也得到了法官和检察官的印证。

图一：案件数量变化示意图

综上所述，虽然北大法宝侵犯个人信息犯罪的数据只是全国该类犯罪

数据的一部分，但已能够大体上反映出我国侵犯个人信息犯罪的整体状况:

首先，公民个人信息犯罪连年迅速增长，涉案信息数量和金额越来越多，危害越来越严重；其次，获取公民个人信息类犯罪占据了该类犯罪的绝大多数，但对于个人信息犯罪的源头，出售和非法提供个人信息获得惩处案件的数量相对较少，不利于从源头上予以打击；再次，和个人信息犯罪呈现愈演愈烈之势形成鲜明对比的是，其量刑却相对较轻，缓刑比例较高，难以有效地预防和惩处该类犯罪的发生；最后，对于个人信息犯罪“情节严重”的标准认定上，无论是涉案信息的数量，还是涉案金额，各个地区各个法院之间都有着不同的认定标准，导致侵犯个人信息犯罪的入刑门槛不统一，量刑尺度不一致，不利于惩处该类犯罪和维护法治的统一。

2.实证分析得出的规律、结论

（1）公民个人信息犯罪案发高，破案率低。当前个人信息犯罪持续高发，跟个人信息违法成本低，犯罪技术含量高有着密切联系，而且个人信息犯罪案件交易途径多样态，特别是当前国家机关内部人员出售和提供个人信息、通过网络途径买卖个人信息占据了一定程度的比例。犯罪人作案手段隐蔽，技术含量高，作为惩处公民个人信息犯罪案件的第一线侦查机关打击出售和非法提供个人信息犯罪侦查成本高，查处难度大。

（2）侵犯公民个人信息犯罪定罪和量刑标准不清晰。主要是办理侵犯公民个人信息犯罪案件中，不同地区，同一地区的不同法院对“情节严重”考量的标准不统一。

三、侵犯公民个人信息犯罪处刑较轻，刑罚惩处力度较弱。从上述表格统计可以看出，在具有代表性的 182 起案件中，因侵犯公民个人信息犯罪被判处有期徒刑缓刑的案件所占的比例为 40%; 单处罚金的案件所占的比例是 6%; 一年以下有期徒刑（含拘役）的案件所占的比例为 78%; 1 年到 3 年有期徒刑的案件所占的比例为 16%。个人信息犯罪和其他侵犯公民人身和财产安全的犯罪相比，处刑相对比较轻，惩罚力度比较弱，某种程度上可能不足以阻碍侵害公民个人信息犯罪的发生。这和民众普遍感受到的侵害公民个人信息的行为非常普

遍，危害有时十分严重形成了鲜明的对比。刑法的惩戒功能在此部分失真。

表二：样本案件个人信息犯罪罪名表（单位：件）

	案例总数	出售、非法提供公民个人信息	非法获取公民个人信息	同时构成出售、非法提供和非法获取公民个人信息	侵害个人信息犯罪（拆分具体罪名后统计到本表左侧三项）与其他罪名并罚
合计	182	14	163	5	7
比例		7.7%	89.6%	2.7%	3.8%

3.完善预防侵犯个人信息犯罪的建议

（1）尽快制定完善的《个人信息保护法》。制定完善的《个人信息保护法》，这是最基本的最全面的保护个人信息的途径和方法。刑法作为保护个人信息安全的最后一道屏障，要充分发挥其预防犯罪惩治犯罪的作用，很大程度上要依靠民事法规和行政法规的前置性规定。为了更好的保障公民个人信息权，必须尽快通过《个人信息保护法》，并对一系列具体问题出台相关细则。

（2）完善全面的个人信息保护系统，加大惩处侵犯个人信息犯罪的力度。通过各个部门的通力合作，做好对个人信息的监控管理，掌握即时动态。或者由政府牵头，设立一个专门管理个人信息的部门。对个人信息的使用情况做好日常管理工作，一旦发现异常情况，及时报告处理，必要时，可以通知公安机关立案调查。同时将滥用情况通知信息主体。

（3）完善对“公民个人信息”的认定。公民个人信息是一个公民存在于社会的诸多行为痕迹的总和，从生理信息如指纹、声纹、虹膜信息，到社会信息如身份号码、社保卡号码、毕业证编码等。随着社会的进步和发展，信息的内容也在不断地扩充着。

由于个人信息一方面属于个人隐私，一方面又与社会的公共生活息息相关，所以个人信息既有私密性又具有一定的公开性。那么刑法

作为最后的保障手段，在确定个人信息的范畴时就要综合考虑个人信息上述两个属性。

（4）进一步明确对“情节严重”的认定标准。我们认为可以从行为目的、行为次数、信息数量、获利情况等来综合认定。在侵犯公民个人信息罪中，认定“情节严重”建议包括以下情形之一：1.获取公民个人信息从事非法活动的；2.侵犯公民个人信息在 1000 条以上的；3.一年内两次非法侵犯公民个人信息的；4.曾因侵犯公民个人信息受过行政处罚又侵犯公民个人信息的；5.侵犯公民个人信息交易金额 1 万元以上或者非法获利 5000 元以上的。

表三：侵犯个人信息犯罪实际判决一览表

省市	案件数量（件）	单处罚金（件）	拘役	有期徒刑6个月到1年	有期徒刑1—3年	缓刑
上海	75	5	13	47	10	20
北京	29	0	2	21	6	12
浙江	27	1	5	18	3	17
广东	18	0	2	11	5	5
河南	13	1	5	5	2	6
河北	12	2	3	4	3	9
安徽	8	2	1	5	0	4
总计	182	11	31	111	29	73

（来源：《检察风云》2016 年第 18 期）

个人信息保护的立法现状

由于诸多原因，我国个人信息保护立法工作明显滞后于时代和社会的发展。直接保护个人信息安全的法律数量很少，有关条款散见于

我国《宪法》、《民法通则》、《行政诉讼法》、《刑法修正案（七）》等法律、法规和最高法院的司法解释中。2003 年国务院信息管理办公室委托中国社会科学院法学研究所个人数据保护法研究课题组起草《个人信息保护法》（专家建议稿），2005 年该专家建议稿提交，标志着正式启动了我国第一部有关个人信息保护的法律《个人信息保护法》的立法程序，但十余年过去，迄今我国还没有一部关于个人信息安全保护的专门法出台。

近几年，我国个人信息保护立法工作取得了一定的进步。全国人民代表大会常务委员会《关于加强网络信息保护的决定》、国务院《互联网信息服务管理办法》、国家互联网信息办公室《即时通讯工具公众信息服务发展管理暂行规定》、《互联网危险物品信息发布管理规定》、工业和信息化部《规范互联网信息服务市场秩序若干规定》、《电信和互联网用户个人信息保护规定》等专门文件陆续出台。我国《消费者权益保护法》和《刑法修正案（七）》等法律法规中特别强调加强个人信息保护。同时，互联网行业在个人信息保护领域做了大量有益的探索，腾讯、百度、阿里巴巴等著名公司不断实践，借鉴吸收了国外优秀互联网企业在个人信息保护方面的好的经验，制定了适合自身发展的个人信息保护措施。

现阶段，我国对个人信息的保护，主要体现在两大方面：一是个人信息的法律保护，即在相关法律法规中设置个人信息保护条款对个人信息加以保护。个人信息的法律保护可以分为法律的直接保护和间接保护。所谓法律的直接保护，即法律法规明确提出对“个人信息”进行保护；法律的间接保护，即法律法规通过提出对“人格尊严”、“个人隐私”、“个人秘密”等与个人信息相关的范畴进行保护进而引申出对个人信息的保护。我国现行法律对个人信息的保护主要体现为间接方式，对个人信息的直接保护是近几年出现的新趋势，说明国家立法、行政、司法机关和社会公众对个人信息保护的重要意义已经有了正确的认识和足够的重视。二是个人信息的自律保护。即通过信息控制人的单方承诺，或特定行业自律规范的承诺对个人信息加以保护。个人信息的自律保护也表现为两个方面，一个是企业通过单方承诺这种市场运作方式对个人信息加以保护，一个是特定行业组织通过

行业自律规范对个人信息

1.确立行业保护标准从而进行保护。

目前存在的主要问题是:

（1） 在个人信息的法律保护方面: （ a） 法律体系上缺乏呼应。尽管近些年来我国颁布了一些有关互联网信息管理和个人信息保护的法律法规，但这些法律法规之间协同性差，不成体系，给人“杂乱无章”、“群龙无首”的感觉，有些条款甚至相互冲突，不利于法律的适用; （ b） 法律适用范围狭窄。目前我国保护个人信息安全的法律法规数量比较有限，有些是针对互联网信息服务等特定行业、特定对象的法规，在国家立法层面缺少一部适用于所有信息控制人的专门的《个人信息保护法》，即上文所讲的“群龙无首”的“首”; （ c） 法律条款轻描淡写。我国现行涉及个人信息保护的法律法规中，大部分条款对个人信息保护问题一带而过，往往没有揭示个人信息保护法应当具备的重要内容，如个人信息保护的立法理由、个人信息保护的基本原则、信息主体的权利、个人信息收集、处理、利用及传递的规则、个人信息保护的执行机制及监督机制等。（ d） 法律可操作性不强。许多法律条款仅规定了对个人信息的保密义务，而没有规定信息控制人如果违背该义务需要承担的法律责任和后果; （ e） 法律保护手段单一。

重“刑事处罚”和“行政管理”，轻“民事确权”与“民事归责”，导致个人信息遭受侵害后，即使侵权行为人最终受到刑事处罚或行政处罚，但信息主体的财产及非财产损失却得不到任何实质性的补偿。

（ 2） 在个人信息的自律保护方面: （ a） 非公共部门个人信息保护意识和水平参差不齐。我国大多数非公共部门个人信息保护意识不强，没有单方向相对人提供个人信息保护政策。除了互联网行业，其他的非公共部门行业也鲜有保护个人信息的行业自律公约。一些大型商业网站已经清醒地认识到个人信息所蕴藏的巨大价值以及个人信息对于信息主体的重大意义，因而为用户提供了相对详细的隐私保护政策，以提振用户使用网络消费的信心。但一些小型网站的个人信息保护状况堪忧，它们非但没有向用户公开相应的个人信息保护政策，反而唯利是图，过度收集、不当利用甚至非法出售用户的个人信

息，给用户造成损失。（ b） 公共部门个人信息管理重义务轻权利。我国许多公共部门还没有完全适应从公共事务管理者向公共服务提供者的角色转变，它们对个人信息的关注多从管理的角度出发，强调个人信息主体提供信息的义务，而忽视个人信息主体就其自身信息所享有的基本权利。各级政府网站上几乎看不到和一些大型商业网站所公布的“隐私政策”类似的文本。随着我国电子政务的逐步推行，政府部门掌握大量公民通过网络提交的方方面面的个人信息，如果缺乏个人信息保护政策和措施，也可能会侵犯个人信息主体的合法利益。

因此，制定并颁行专门性的《个人信息保护法》，有利于体系化当代中国个人信息保护的相关立法实践成果，提高个人信息保护在我国立法体系中的地位，有助于严厉打击、禁止非法收集和使用个人信息的行为，保障信息的有序、自由流动，有益于我国信息行业和产业的健康发展，对于推动我国当前和未来从网络大国向网络强国迈进，进一步提升经济发展和社会治理水平，具有十分积极的作用和重要的意义。（来源：《北京邮电大学学报》2016 年第 8 期）

个人信息立法保护需明确的基本问题

个人信息立法保护必须明确下述几个基本问题:

1.明确保护对象

个人信息作为法律保护的客体，应该明定范围。在我国目前个人信息的分散立法保护中，基本上个人信息保护并不是上述统计的规范性文件的主要立法目的，只是鉴于个人信息现实保护的需要而加以附带规定。所以多数规范性文件中没有明定何为个人信息，只是简单作了应当保护个人信息的原则规定。这个问题有必要专门统一解决，但结合已有的立法经验，如何界定个人信息需要考虑如下问题:

其一，个人信息的基本内容列举。在上述统计的分散保护个人信息的规范性文件中，列举的个人信息有姓名、住址、身份证号码、职业、消费情况、联系方式等个人社会交往信息；出生日期、性别、指纹等生物特征信息；收入和财产状况、银行账号等财产信息；健康状况、就医等医疗信息。而在专门保护个人信息的规范性文件中，增加了基因、血型等生物特征信息；疾病、病史等医疗信息；存款、有价

证券、商业保险、不动产、纳税数额等细化的财产信息；婚姻状况、职业经历等社会信息；犯罪记录、不良信用记录等负面信息；宗教信仰、私人活动等其他信息。综合起来看，几乎包含了从生物特征、社会交往、财产、医疗、私人信仰、私人活动等较为全面的个人信息，但总体上，列举的内容以泛泛的社会交往信息最为常见。在未来的个人信息立法中，上述出现的具体个人信息都值得关注，但需要从明确分类的角度总结已列举的内容，决定是否列举以及如何选择列举的具体内容。

第二，可识别个人性的概括界定。《统计法》、《规范互联网信息服务市场秩序若干规定》、《侵害消费者权益行为处罚办法》中出现了“能够单独或与其他信息结合识别用户的信息”的概括规定，这与专门立法保护中的概括规定一致。可以说，“可识别个人性”是信息与个人相连，并能够最终与侵犯个人权益相结合的最基本特征。但值得注意的是，《决定》及《解释》中出现的涉及个人隐私也是个人信息概括规定的一个标准，其如何与个人识别性相结合判断个人信息还是一个需要认真研究和论证的问题。

第三，敏感个人信息的保护问题。敏感个人信息和个人隐私保护紧密相连，直接关涉个人人格尊严的维护，张新宝教授就提出了“我国未来个人信息保护法应当以‘个人敏感隐私信息’概念对个人信息进行类型化区分”的主张。何为敏感个人信息？如何明确保护范围？除了上述列举的种类外，其他国家立法中的犯罪记录、政党派别以及社会团体成员身份等敏感个人信息能否为我国借鉴？这些问题都需要结合我国的文化传统和社会实际专门进行研究。

2.具体化个人信息处理原则

个人信息保护原则是个人信息立法的核心内容，1995 年欧盟数据保护一般指令就确立了合法、终极、透明、合适、保密和安全及监控原则，这六大原则目的是在提供数据保护最低限度制度基础上促成数据的自由流通。这六大原则也成为世界范围内各国个人信息立法保护的基本原则。与之相比较，六大原则已经存在于我国的规范性文件中，只是具体内容并不详实。最主要的问题是各规范性文件中原则规定不统一、具体制度设计并没有发挥原则的指导作用，从而导致个人信息

保护的分散与随意性。

3.准确定性个人信息主体的权利

个人信息主体权利作为个人信息法律保护的核心内容直接对应个人信息处理主体的义务并与个人信息法律保护责任相匹配。所以必须从法律保护的权益目的出发明定个人信息主体权利。

目前，更多学者认为，个人信息保护的是人格权，兼具隐私、财产双重权益属性。个人信息主体的权利作为个人信息立法保护的核心问题，其辐射影响信息业者和国家利用及监管个人信息的权益和义务。各国立法中，通常直接确立个人信息自决权，这是个人信息隐私权属性的具体体现，有学者论证认为，从权益损害的角度看，个人信息买卖能够获利是个人信息泄露、滥用的驱动力，而对获利性的法律惩处并不等同于对个人信息财产权的保护，因为，大数据时代，往往大量的个人信息聚集才会产生财产利益，个人信息仅是这种社会财产权的微小组成部分，个人无法通过个人信息财产权主张完成对自身权益保护的主张。总之，个人信息权利属性是与个人隐私权保护密切相关又有区别的，但显然，由于目前我国个人隐私也没有明确的法律保护，在立法实践中，两者的关系如何理清、个人信息权利如何定性及如何进行利益平衡等还需认真研究论证。

4.落实个人信息保护法律责任

法律责任承担是法律权益保护的直接实现，目前我国规范性文件中个人信息保护法律责任规定虽然类型全面，但是普遍存在无法落实的困境。原因主要在于没有明确规定个人信息与个人信息权利内容，致使法律责任缺失具体侵权依据，无法进行危害程度和危害结果的量化规范。于是，在法律责任规定上，多数采取“泄露用人单位和个人信息的，依法给予处分或行政处罚”的简单宣示规定，或者泛泛规定“造成损失”、“侵犯合法权益”的，承担民事赔偿责任，构成犯罪的承担刑事责任等。具体在刑法修正案中，由于保护的个人信息内容不详、证据认定和量刑标准模糊，使得刑事责任的规定并没有发挥打击个人信息滥用、个人信息买卖的功效.法律责任是个人信息保护的最后关卡，无法实际落实正暴露了个人信息保护的无力和不足，这一最后防线需要在个人信息立法内容明确的基础上进行精心设计。（来源:

《东方法学》2016 年第 3 期）

《个人信息保护法》立法的原则和建议

1.我国《个人信息保护法》立法应坚持的原则

首先，坚持公开收集原则。“公开”并非指个人信息内容的公开是指个人信息收集、存储、利用及提供等相关情形公开，保障信息主体的知情权。政府或企业在收集公民个人信息时，应当向其告知有关信息收集的目的、使用范围等情况。

其次，坚持利益平衡原则。在信息社会，信息作为战略性资源，其自由流动具有重要的基础性意义。因此，必须协调好个人信息保护与促进信息自由流动的关系，平衡好个人信息保护与行业发展的关系，避免左支右绌，顾此失彼。

再次，坚持国际接轨原则。当前世界各国之间的司法合作越来越频繁，各国立法实践中的有益成果应该共享。我国立法既要立足我国的具体国情，也要主动适应国际化需求。在个人信息保护方面，各国已经逐渐认识到了传统隐私权法律保护的不足，隐私权的内涵也已从消极被动的“私生活不受干扰”的人格性权利发展为积极能动的“自己的信息自己控制”兼具人格和财产属性的权利，即个人信息自决权的概念。我国的个人信息保护法也要顺应这一变化，保障个人信息主体的自决权，包括信息保密权、信息选择权、信息查询权、信息更正权、信息禁止权、报酬请求权、损害赔偿请求权等。

2.我国《个人信息保护法》立法的具体建议

（1）明确个人信息收集目的。个人信息管理者不应在个人信息主体不知情、未参与的情况下采取隐蔽技术手段或采用间接方式收集个人信息。收集个人信息前应当向个人信息主体明确告知如下事项：（a）收集个人信息的目的、使用范围和收集方式；（b）个人信息管理者的名称、地址、联系办法；（c）不提供个人信息可能出现的后果；（d）个人信息主体的权利；（e）个人信息主体的投诉渠道。

个人信息管理者不得收集与其所告知的信息收集目的无直接关系的个人信息，特别是揭示个人种族、宗教信仰、基因、指纹的信息，

或与健康状况、性生活有关的信息。

（2）加大对未成年人等特殊群体的保护。对未成年人的个人信息采取特殊保护是世界各国的通行做法。当个人信息管理者发现个人信息主体未满 16 周岁时，应给出明确提示并停止收集行为，为提供必要服务确需收集其个人信息的，应征得其监护人的同意。收集或取得未成年人的个人信息手段，包括但不限于要求未成年人提供在线个人信息； 通过聊天室、留言板或其他方式使未成年人信息暴露在公共场合； 此外还包括消极地追踪或者使用其他方式，如 cookie 确定其个人身份代码。

（3）增设个人信息主体的自主选择权和控制权。个人信息主体的自主选择权是指个人信息主体本人有权选择是否向相关信息管理者提供个人信息以及是否允许相关信息管理者向其收集个人信息；个人信息主体的控制权主要表现为对个人信息的使用、修改或删除的权利。个人信息主体的自主选择权和控制权是个人信息保护的重要手段，既可以保证个人信息的收集获得信息主体的授权，也可以更全面地保证个人信息的使用的安全。

（4）强化数据泄露通知制度。2011 年底前后，因云计算等新业务的发展和亚马逊等公司数据事故的发生，美国开始着手拓展数据泄露通知制度。2012 年，欧盟个人信息保护立法改革，提出引入数据泄露通知制度。我国未来《个人信息保护法》应当明确，一旦发生数据丢失、被窃，或者遭遇未经授权的接入，致使敏感的、可识别个人身份的数据信息的机密状态、完整状态存在受损可能的情形，相关责任主体需在一定时限内向受损主体或有关执法主体进行通告。

（5）明晰云计算大数据的使用权限。随着大数据和云计算的普及，促使大量的个人数据收集和分析成为可能，政府和企业的决策越来越依赖大量的数据收集和分析。在这种情况下，数据挖掘、分析技术使数据被利用的可能性增加，数据被收集、使用的安全风险增大。我国未来《个人信息保护法》应当从立法上明晰个人隐私与公共信息涉及的不同范围界限，明晰公权力进入个人隐私范围的界限，明晰哪些公共信息属开放、共享的范畴。

（6）强调智能终端 APP 个人信息保护。中国互联网已进入移动互

联网时代。《个人信息保护法》应当对移动 APP 产业链上的相关主体提出针对性条文，明确移动 APP 开发者必须遵循以下规定： 提供易懂、易得的隐私政策； 对及时披露收集和处理的数据，取得用户明确、知情授权； 告知用户修改、删除、拒绝等权利； 在 APP 设计和实施各个阶段进行隐私设计确保安全。

（7）建立统一的个人数据保护机构。成立专门负责个人数据保护的机构是各国的普遍做法。我国目前还未建立专门统一的个人数据保护机构，各部门是在传统的监管职责中延伸管理各自行业、部门的个人信息保护问题。但从长远发展来看，建立专门机构有利于监督《个人信息保护法》的落地，提升整个国家的个人数据保护水平，也有利于对各行业、各部门的个人数据保护履行监督管理职责，更有利于为用户（ 个人信息主体） 建立维权申诉的一站式服务。

（8）设立个人数据跨境监管制度。我国未来《个人信息保护法》应当规定： 对涉及到国家安全等重大国家利益的个人数据禁止转移到国外；将用户个人数据转移至境外，应当取得用户的明确同意；国家制定数据跨境转移的合同范本，指导企业跨境转移活动； 对于将个人数据转移至他国，提供给他国政府的，应当取得数据保护机构的同意。（来源： 《长春邮电大学学报》2016 年 6 期）

大数据时代政府对个人信息的保护问题

信息时代，在计算机和互联网等技术的推动下，公民个人信息的收集、存储和传递逐步数字化，个人信息成为政府管理、社会服务和商业拓展的重要手段与资源。作为社会管理者和公共服务的提供者，政府是一国最大的信息生产、收集、使用和发布单位。一些政府部门在收集、利用、公开和整合利用信息时存在侵犯公民个人信息隐私的问题，给受害者带来不同程度的困惑甚或是危害。因此，如何保护个人信息是每一个政府不得不考虑的问题。

大数据时代政府部门侵犯个人信息权利的隐患

随着信息化和大数据的发展，政府作为个人信息最大的消费者，掌握着大量的个人信息，个人信息隐私权面临来自政府部门在收集、

公开、管理、利用等各个环节的侵犯危险。

1.一些政府部门在收集数据时存在侵犯个人信息隐私的问题。

由于我国个人信息隐私权保护观念滞后，在行政权力行使惯性的背景下，一些政府部门在收集数据时侵犯个人信息隐私的行为经常发生。比如：2013 年 10 月 11 日，山东滨州学院因为宿舍失窃，只为揪出学生宿舍里的小偷，学院五千多名本科男生全部被采血验 DNA。DNA 数据是公民的敏感信息，公安局如此执法确有轻率和滥用权力之嫌。但也应该注意到，目前我国对 DNA 的采集范围和程序无法可依，才会出现上述公然侵犯公民个人隐私权的事件。下面以我国政府的两大工程为例，进一步说明政府收集数据侵犯公民隐私的情形。

在互联网、信息技术发展和行政权力扩张的推动下，各国均进入建立巨型统一个人信息数据库时代。我国从 2004 年 1 月在上海市、江苏省扬州市和湖南省启动人口基础信息共享试点；“自 2007 年开始，我国开始整合政府各部门的人口信息资源，以公安人口信息为基础，逐步融合计划生育、统计、民政、社会保障、税务、教育等部门的相关信息资源”。在政府巨型数据库面前，公民几乎完全没有个人隐私。从政府信息化直到巨型数据库建设，我国都采用政府权力推进的方式，没有公民的参与，也没有人大立法的监督。由此导致巨型数据库建设更多考虑的是行政效率和管理方便，对于公民隐私权尤其是个人信息保护的观念和制度设计缺失。

2.一些政府部门在公开数据时存在侵犯个人信息隐私的问题。

政府是掌握最多信息的机构，拥有整个社会信息资源的 80%，其中包括大量个人信息。而目前各国都致力于建设一个公开、透明的政府。美国总统奥巴马于 2008 年就任日发表一份备忘录，声称要建立一个前所未有的开放政府，同时命令联邦机构的负责人全面公开所掌握的信息。之后美国建立联邦政府公开信息资料库 data.gov 网站，截至 2012 年 7 月，网站的数据集已达 45 万个，涵盖美国 172 个机构。2011 年 9 月，美国、英国、挪威、墨西哥、印度尼西亚、菲律宾、南非等 8 个国家共同发起了一个新的国际组织：开放政府联盟（OGP），该组织承诺要通过互相监督、共同努力来推动世界各国政府的信息公开工作。目前，该组织已经有 53 个会员国。我国 2008 年 5 月 1 日开

始实施《政府信息公开条例》，要求政府信息公开。从开放走向透明代表的是数据民主权利的行使，是政府满足公众知情权、公开其所掌握的信息的阳光举措。政府信息公开有助于公众了解政府的作为，提高政府的工作效率，促进政府更好地履行职责并建立问责制。

但是，政府在公开这些信息的过程中必然会涉及对公民个人信息的公开，从而存在侵害个人信息隐私的危险。我国《政府信息公开条例》虽然对信息公开的范围、方式、程序和监督等问题作出规定，同时该法第 14 条第 4 款也规定: “行政机关不得公开涉及个人隐私的政府信息。经权利人同意公开或者行政机关认为不公开可能对公共利益造成重大影响的涉及个人隐私的政府信息，可以予以公开。”这一规定非常笼统，既未对“个人隐私”的范围进行界定，也没有对何为“公共利益”，何为“重大影响”作出明确解释。由此引发许多争执，比如公安机关根据处罚公开原则，将交通车辆监控到的不雅视频曝光，将处罚结果公开曝光，76%的网民认为侵犯处罚相对人的隐私权。在大数据时代，政府由于其特殊地位，获取个人信息的数量和真实性都与其他收集主体不同，一旦过度披露个人信息，对公民权益的危害更为严重。

3.一些政府部门在数据管理中存在侵犯个人信息隐私的问题。

我国相关法律对政府工作人员保守执业秘密均有规定，但政府工作人员出售、非法提供个人信息给无权获取者的现象日趋严重。中国青年报 2011 年调查“公民个人信息是如何泄露的”，86.5%的公民认为自己的个人信息曾被泄露，受访者认为在泄露自己信息可能性的部门与机构中，政府为 24.9%、教育为 24.3%、银行为 39.8%、保险公司为 37.0% 。被泄露的信息从姓名、性别、出生时间、住址、婚姻、身份证号码等个人户籍资料，到学历、职业、生活经历、车辆档案信息、公司工商档案、出入境、旅客住宿记录、财务状况，甚至包括血型、指纹、病历、生育状况等。

4.一些政府部门在利用数据时存在侵犯个人信息隐私的问题。

政府出于特定目的收集的分散的个人信息，被整合与利用的数据挖掘，是大数据时代个人信息保护面临的最大挑战。即使最初政府收集个人信息经过个人许可，但现有大数据处理技术可以很容易地实现

政府信息化的全面整合或无缝衔接。如果政府暗自将分散在各行政机关数据库的个人信息进行整合，形成新的信息，完全没有经过个人的许可和其他监督，极容易侵害公民的权益。

大数据时代我国政府保障公民个人信息权利的对策

当我们风驰电掣地进入大数据时代，政府作为一国最大的信息数据消费者、信息收集使用的监管者，却未能充分做好迎接它的准备。根据前文的分析，以发展的眼光考量，需要从以下方面对政府保护个人信息的策略提出展望。

1.强化政府人员保护个人信息隐私的意识。

我国是生产个人信息最大的国家，因为我们人口最多，但政府相关人员却缺乏保护个人信息的意识。应加大培训、教育力度，使相关人员了解：进入大数据时代，个人信息的外延不断地扩展，无论是个人的静态识别信息，还是其动态的私人活动信息；无论是个人不愿公开的敏感信息，还是其选择公开的生活琐事信息，都应当属于受保护的个人信息范围。因为，个人要在信息社会生存，无法不交出自己的信息。但交出这些信息，并不等于放弃其隐私权保护，公民有权利要求基于特定目的获得个人信息的政府机关、单位遵守信息伦理，按照国家法律规定，妥善使用、保管信息，不得随意滥用和泄露个人信息。

在推动政府保护个人信息的进程中，对自己信息权益最为关心的公民起着重要作用，日本“住基网络诉讼”便是例证。日本政府根据相关立法，开通收录全体国民确认信息的巨型数据库——“住民基本台账网络系统”（简称住基网络），使全国各级行政机关实现数据共享。这遭到日本部分国民的反对，他们以个人信息隐私权受到侵害为由，陆续提起三十多起诉讼。通过诉讼，日本最高法院明确，收集和利用个人信息的前提是“有比较完善的个人信息保护法律制度和技术措施，禁止个人确认信息的目的外使用”。由此可见，政府强化保护公民个人信息的意识与举措，是政府与公民社会博弈的结果，是协商式民主的成果。

2.尽快出台个人信息保护法。

个人信息在政府掌控之下，并面临着政府公开的威胁，由此要求

制定法律规范行政机关收集、利用和传播个人信息的行为，保证政府收集个人信息的正确性，并不得滥用个人信息。虽然我国在收集、使用和传播个人信息的技术上有突飞猛进的进步，但个人信息保护的法律制度与此并不匹配。除了零星法律规范中的原则规定和行政机关制定一些内部工作规范，缺乏一部全面完整系统保护个人信息的法律。因此必须尽快出台“个人信息保护法”，明确界定个人信息的范围；明确行政机关收集、使用、管理个人信息的范围，政府保护个人信息的职责和义务；明确“公共利益例外公开”的界限等。

3.加强政府内部管理。

政府对其工作人员接触个人信息，应当建立完善的管理制度，保证个人信息处于安全保护中。首先，各行政机关应当明确工作人员的权限范围，控制接触具体个人信息的人员。这样可以减少对个人信息的随意接触，从源头上避免泄露公民个人信息。其次，对于必须接触个人信息的工作人员，严格设置进入数据库的登记制度，实时监控进入数据库的行为。第三，制订规则，设置必要的保护措施，不能随意下载数据。通过明确工作人员的权限范围，即使出现个人信息泄露现象，也能及时发现泄露的渠道。通过设定完备的操作程序，避免因为违反操作规程造成个人信息的泄露，从而侵害他人的合法权益。

4.加强政府监管职责。

传统的个人信息保护模式，强调本人对自己信息的知情、控制和支配权利。但大数据时代，数据的价值主要体现在整合利用上，收集数据时“告知与许可”模式已不能适应时代的需求，应该更注重数据使用者为其行为承担责任。政府向全社会公开所掌握的数据，在数据公开之前，政府负有保护数据库中个人隐私的责任和义务。比如在公共部门信息公开网站公布含有个人隐私数据时，隐去数据中关涉个人隐私的痕迹。政府为了公共利益或商业利益允许其他机构使用政府信息库，我们可借鉴美国的做法，涉及隐私信息的数据集，如出生、死亡、结婚和离婚等数据集时，只提供统计数据而不能看到元数据。

政府应加强对其他机构与人员授权利用个人信息的管理，对于利用数据库的其他社会组织，因为处理海量数据而知悉个人信息，负有保护个人信息隐私的责任，即谁利用谁负责，政府承担监管职责。“我

国在政府信息增值利用中的个人信息保护立法相当薄弱，可借鉴欧美对于信息利用前、中、后三个阶段进行信息保护法律规制”，通过加强对监管内容和监管对象行为的规制，达到保护个人信息隐私权的目的。

另外，在我国当前情况下，还需要完善侵害个人信息权利的救济体系。“无救济则无权利”，信息社会个人信息隐私的权利救济是保障其权益实现的有效途径。建立以行政责任和民事责任为主，刑事责任为辅的多重救济模式。这种救济体例，使得各法之间互为照应。在我国，从侵权法角度救济个人信息隐私利益，公民可以通过民事诉讼途径实现。但是依据现有的行政诉讼法，公民针对政府行政行为侵犯个人信息隐私权的诉讼，尚没有明确的法律依据。由于政府监管不力，导致其工作人员或其授权使用个人信息的机构与他人，侵犯个人信息隐私权时，立法应当赋予个人信息主体通过复议和诉讼救济其权利。最后，当行政责任、民事责任适用无效，可运用刑罚手段加以惩罚，体现刑法作为最后底线的权利救济措施。（来源：《理论探索》2015 年第 2 期）

国外个人信息安全的保护策略

国外个人信息保护立法进展

随着社会与科技的发展，20 世纪 70 年代在欧美国家兴起了大规模制定个人信息保护法的热潮。

全球第一部以“资料（也有译为“数据”）保护法”命名的法律是 1970 年的德国《黑森州资料保护法》，虽然它只是州层面的立法。瑞典于 1973 年通过了《资料法》；奥地利于 1978 年通过了《联邦资料保护法》；1977 年，德国联邦政府颁布了《联邦资料保护法》，将联邦层面的个人信息保护问题进行了统一规范。此后，德国又对该法进行了修订，形成了《1990 年联邦资料保护法》和《2001 年联邦资料保护法》。由于欧盟各成员国对个人信息保护的标准并不统一，1995 年欧盟出台了《数据保护指令“Directive95 /46 /EC on the protection of individuals with regard to the processing of personal data and

onthe free movement of such data”》（全称《欧洲议会和欧盟理事会 1995 年 10 月 24 日关于涉及个人数据处理的个人保护以及此类数据自由流动的指令》），为个人信息保护提供了全方位、综合性的保护。《数据保护指令》1998 年生效并对各成员国具有强制效力，要求成员国修改本国的数据保护法以执行其有关个人数据保护的规定。2012 年 1 月 25 日，欧盟又出台了《欧洲数据保护法案“European Data Protection Regulation”》。美国 1974 年颁布了《隐私权法“Privacy Act”》，1986 年又颁布了《电子通信隐私法“The Electronic Communication Privacy Act”》（简称 ECPA）。

目前全球已有 60 多个国家制定了专门的个人信息保护法。从立法模式上看，主要有 3 种：一是美国模式，将分散立法与行业自律相结合，在公共领域制定单行法律进行分类保护，如 1998 年的《儿童网上隐私保护法》；在私人领域采取行业自律模式，在政府主导下制定行业准则，通过自我约束保护公民的个人隐私。二是德国模式，在公私领域对个人资料采取统一立法模式进行保护，如它既有统一的《联邦资料保护法》，又有适用于所有州个人信息保护的《州资料保护法》，并设立独立的监督机构。

三是日本模式，采取综合性的保护模式，兼具统一立法规制和行业自律特点，如 2005 年日本《个人信息安全保护法》作为个人信息安全保护的基本法律对公私领域进行统一保护，并分别针对不同部门、特殊行业制定个法，形成以《个人信息安全保护法》为基本法，各部门单行法为补充的法律体系。以上 3 种模式侧重点不同，但都有其合理性及局限。美国模式相对灵活，在保护个人隐私的同时能够促进信息的流通，规定具体而可操作，但容易造成司法的不统一。德国模式具有规范性和强制性，有利于对个人信息安全的全面保护，但难免僵化，不利于个人信息的充分流动，影响企业和社会的发展。日本模式是前两者的折中，具有宽泛性和适用性，但对保护对象和规制对象定义不严谨，反而影响了正常的信息交流。在我国个人信息保护立法中，应全面、辩证地分析上述 3 种立法模式的得失，取长补短，兴利除弊。（来源：《民主与法治》2016-08-19）

国外个人信息安全保护典型经验和做法

美国、欧盟等建立较为完善的信息安全保护法律体系

美国制定了一系列信息安全保护的法律，加强个人信息安全保护。1966 年美国国会颁布了《信息自由法》，这是美国在信息安全领域立法的起点。1974 年出台的《隐私权法》明确规定了信息公开与隐私保护的处理规则。1986 年出台的《电子通信隐私法》对政府拦截监听通信信号的范围与标准等做了相关规定。之后美国先后制定了《计算机安全法》（1987 年）、《通信净化法》（1996 年）、《数据保密法》（1997 年）、《网络电子安全法案》（1999 年）、《网络安全信息法》（2000 年）、《网络安全法案》（2009 年）等 20 余部法律，以上这些法律均由美国最高立法机关国会制定，构成了美国最基本的信息安全法律体系框架。

欧盟在欧洲议会、欧盟理事会和成员国的共同努力下，不断制定和完善信息安全法律法规体系。例如，1981 年通过了《有关个人资料自动化处理保护个人公约》，1995 年欧盟制定了《个人数据保护指令》以保护个人数据及其自由流动，2002 年通过了《关于电子通信行业个人数据处理与个人隐私保护指令》等，此外还出台了一系列指令、决定、决议和公约。

美、英、日、德等国普遍建立信息安全国家战略

美国：美国在全球互联网领域拥有绝对的控制权和主导权。2009 年发布了《网络空间政策评估---保障可信和强健的信息和通信基础设施》，2011 年发布了《网络空间国际战略》进一步确立了其战略意图。

英国：英国于 2009 年颁布了《英国网络安全战略》，着眼于从宏观长远角度加强网络安全建设，维护本国网络安全。

日本：日本于 2005 年组建了跨越陆海空的“网络战部队”。2006 年、2009 年先后发布了《第一个国家信息安全战略》、《第二个国家信息安全战略》，2011 年发布了《保护国民信息安全战略》，2013 年制定了《网络安全战略》，同时组建了“网络防卫队”。

德国：作为欧洲信息技术最为发达的德国，高度重视网络信息安全建设。1997 年就发布了世界上第一部计算机网络服务方面的单行法律---《多媒体法》，2011 年发布了《德国网络安全战略》，成立了

国家网络防御中心，建立了国家网络安全委员会。

美国在互联网领域具有独特的优势，在全球 13 个根域名服务器中占据了 3 个，拥有全球最大的网络带宽，拥有最大用户数量的信息服务以及领先的软硬件核心技术。以 Microsoft、IBM、Apple、Google、Intel、Oracle、Cisco 等为代表的信息巨头公司在全球信息安全产业中占据着基础性的关键支撑作用，改变着全球用户的工作和生活方式。以 Symantec、Trend micro 等为代表的信息安全产业巨头引领着全球信息安全产业发展。（来源：《人民日报》2016-08-26）