冯占英，陈　锐，张　玉，等. 公民个人信息泄露问题现状分析及对策[J]. 中华医学图书情报杂志，2022，31(6)：9-19.

DOI：10.3969/j.issn.1671-3982.2022.06.002

·研究与探讨·

公民个人信息泄露问题现状分析及对策

冯占英[1]，陈　锐[2]，张　玉[1]，王　妤[1]，郑　斐[1]，张建平[1]，李　璐[1]

[摘要]针对公民个人信息泄露高发问题，调研了国内外典型的个人信息泄露案例和相关研究文献，总结了公民个人信息泄露的被动收集性、群体参与性、集体博弈性、平衡对立性、连锁反应性和时间滞后性等特征，分析了公民个人信息泄露的 4 个主要途径，剖析了个人信息泄露的原因，并对公民个人信息安全防范提出建议。

[关键词]个人信息；信息泄露；隐私；信息安全

[中图分类号]G203　[文献标志码]A　[文章编号]1671-3982(2022)06-0009-11

Status quo of citizens′ personal information leakage and research on countermeasures

FENG Zhan-ying[1], CHEN Rui[2], ZHANG Yu[1], WANG Yu[1], ZHENG Fei[1], ZHANG Jian-ping[1], Li Lu[1]

（1.Library of Academy of Military Sciences, Beijing 100039, China; 2. Information Research Center of Military Sciences, Academy of Military Sciences, Beijing 100142, China）

Corresponding author: ZHANG Yu

[**Abstract**] In view of the high incidence of citizens′ personal information leakage, typical leakage cases and references at home and abroad were investigated. The characteristics of citizens′ personal information leakage were summarized into passive collection, group participation, collective game, balanced opposition, chain reaction and time lag. Four main ways and the causes of citizens′ personal information leakage were analyzed and suggestions were made for citizens′ personal information security.

[**Key words**]Personal information; Information leakage; Privacy; Information security

大数据环境下，信息及数据技术的发展极大方便了人们的生产生活。但技术为人们带来便利的同时，也引发了个人信息泄露问题。个人信息泄露案件呈逐年高发态势，并且随着数据价值的增加，其影响也越来越大，公民个人信息隐私保护引起了大家的广泛关注。本文主要针对公民个人信息安全问题，通过分析典型案例，剖析其产生原因，提出相应的对策。

1　公民个人信息泄露问题研究概述

近些年，众多学者对公民个人隐私问题开展了研究，内容主要集中在个人信息保护相关法律、各领域的个人信息保护策略研究、个人信息泄露分析研究和个人信息保护技术等。

1.1　个人信息保护相关法律研究

为了保障个人信息的隐私保护和数据安全，许多国家和地区制定了与个人信息保护相关的法律

[作者单位]1.军事科学院图书馆，北京　100039；2.军事科学信息研究中心，北京　100142

[作者简介]冯占英（1973-），女，博士，研究馆员，馆长，研究方向为知识组织、领域服务及数字图书馆研究等。

[通讯作者]张　玉（1983-），女，硕士，副研究馆员，副馆长，研究方向为知识组织、数字图书馆。E-mail：zhangyu3417@126.com

法规和政策[1]。

1.1.1 欧盟

1995 年，欧盟通过了《数据保护指令》，以最低保护限度为要求，协调了各成员国在数据保护上的一致性，由于该指令原则性强、实际操作性弱，实践中各成员国多通过国内立法对其进行解释，而成员国立法混乱，导致数据壁垒形成，严重阻碍了数据流通。为了适应互联网和大数据的快速发展，欧盟于 2018 年出台了史上最严格的《通用数据保护条例》。该条例不仅仅适用于欧盟，也适用于为欧盟境内的个人提供商品、服务，以及收集欧盟公民个人数据的企业，管辖范围几乎涉及全球。该条例为成员国的数据立法提供了统一标准，建立了健全完备的监管机制，对个人信息给予了全面保护。总体而言，欧盟认为个人信息属于基本人权，以综合立法的形式确定各成员国的个人信息保护标准，侧重政府公权力的介入。

1.1.2 美国

1974 年，美国通过了《隐私法案》。该法案规范了联邦政府处理个人信息的行为，但对州政府或私营企业没有约束力。之后，美国各州陆续出台了相应的数据隐私法案，如《加利福尼亚州消费者隐私法案》《加利福尼亚州隐私权利法》《弗吉尼亚州消费者数据保护法》《科罗拉多州隐私法》等。在商业领域，美国采取分散立法的模式，制定了《信息自由法》《网络安全信息共享法》《驾驶员隐私保护法》《电子通讯隐私法》《儿童在线隐私保护法》等针对特定领域的单行行政法，使个人信息保护立法得到不断完善。总体而言，美国认为个人信息属于个人隐私，以分散立法的模式来限制政府对个人信息的获取，主张个人数据跨境自由流动，强调行业自律和政府辅助监管。

1.1.3 中国

2013 年，中国工业和信息化部出台了《电信和互联网用户个人信息保护规定》，明确了电信业务经营者、互联网信息服务提供者收集、使用用户个人信息的规则；2016 年，《中华人民共和国网络安全法》把个人信息保护纳入网络安全保护范畴，明确规定了违反个人信息保护应负的法律责任；2021 年，全国人大常委会先后通过了《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》，真正实现了个人隐私与信息保护综合立法“零”的突破。总体而言，我国采取宽严相济的立法模式[2]，在明确个人在个人信息处理中的权利的基础上，采取行政干预方式，对国家机关个人信息处理者的行为进行规范。

我国学者从各个方面对个人信息保护的相关法律进行了研究。有学者研究了大数据背景下个人信息安全法律问题[3]，有学者研究了大数据时代保护个人信息的行政法[4]，有学者从民法角度研究了大数据时代个人信息保护策略[5-6]，有学者研究了公民个人信息的刑法保护法律完善问题[7]，有学者研究了网络环境下个人信息保护的行政监管[8]，有学者研究了关于 App 收集个人信息的行政法规制度[9]等。这些学者从不同角度和层面研究了我国个人信息保护的相关法律，客观上推动了我国个人信息保护法规的建设。

1.2 多个领域的个人信息泄露研究

个人信息内容众多，涉及行业范围广，不少领域都存在个人信息泄露风险，国内不同领域的学者对此进行了相关研究。如有学者研究了电子支付中的个人信息保护问题[10]，有学者研究了个人生物识别信息的隐私权保护策略[11]，有学者研究了疫情防控背景下个人信息的安全问题及对策[12]，有学者研究了网上银行的信息安全保障义务[13]，还有多位学者对电商背景下的快递服务用户信息、民航旅客信息、在线旅客个人信息泄漏情况及对策进行了思考[14-17]，有学者讨论了大数据趋势下的搜索引擎用户的信息安全[18]。

1.3 个人信息泄露分析及治理研究

不少学者针对个人信息的泄露途径及泄露行为进行分析，并提出了应对策略。如有学者对内幕交易者的信息泄露行为进行了分析[19]，有学者研究了个人隐私泄露的途径与防范措施[20]，有学者对大数据时代个人隐私数据的泄露进行了

调研与分析[21]，有多位学者对我国公民个人信息保护现实困境与对策、大数据分析的隐私信息保护方法、公民个人信息安全防控体系、人工智能时代的个人信息安全挑战与应对等[22-26]问题进行了研究。

1.4　个人信息保护技术研究

随着互联网应用的普及和人们对互联网的依赖，个人信息泄露事件频发。大数据、云计算等技术的发展更加剧了这一现象。针对个人信息保护技术，有关学者进行了研究。如有学者研究了个人信息泄漏检测模型的对抗攻击策略[27]，有学者探讨了基于计算机技术对涉密信息的保护[28]，有学者研究了面向边缘计算的任务卸载隐私保护技术[29]，有学者设计并应用了基于数据流的 Android 应用信息泄露检测平台[30]，有学者研究了位置大数据中基于隐私保护的加密技术[31]，有学者对大数据时代个人隐私保护路径进行了重构[32]，有学者研究了基于矩阵变换的大数据隐私保护关键技术[33]等。但总体而言，个人信息防护技术的研究滞后于信息技术的研究。

1.5　个人信息理论研究

由于个人信息大多为被动收集，大多时候公民在享受信息便利的同时也丢失了个人信息。数据的共享与隐私保护、个人信息保护也涉及伦理问题。有学者研究了大数据的“共享-隐私”悖论[34]，有学者研究了大数据发展与隐私保护问题[35]，有学者分析了大数据语境下个人信息隐私安全伦理[36]。

本文通过调研公民个人信息泄露现状，分析公民个人信息泄露特征，剖析泄露途径和原因，探讨公民个人信息泄露的防范措施。

2　公民个人信息概念及范围

在我国，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”。在我国现有法律体系中，已有多部法律法规对个人信息做出了定义，如《中华人民共和国网络安全法》第七十六条、《中华人民共和国民法典》第一千零三十条及 2021 年 11 月 1 日起施行的《中华人民共和国个人信息保护法》第四条等。《中华人民共和国民法典》《中华人民共和国网络安全法》等相关法律列举了个人信息的范围，主要包括自然人的姓名、出生日期、身份证件号码、生物识别信息、住址、电话号码、电子邮箱、健康信息、行踪信息等。为了进一步细化相关信息，国家标准化管理委会于 2020 年 3 月 6 日发布了《信息安全技术个人信息安全规范》（GB/T 35273-2020）[37]，列举了个人信息的主要范围，包括个人姓名、生日、性别、民族、国籍家庭关系、住址、个人电话号码、电子邮件地址等个人基本资料，身份证、军官证、护照、驾驶证、工作证、出入证、社保卡、居住证等个人身份信息，个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部识别特征等个人生物识别信息，以及网络身份识别信息、个人健康生理信息、个人教育工作信息、个人财产信息、个人通信信息、联系人信息、个人网上记录、个人常用设备信息、个人位置信息、其他信息等。

3　公民个人信息泄露案例及特征分析

个人信息泄露案件呈逐年高发态势，并且随着数据价值的增加，其影响也越来越大。本文通过梳理 27 起影响较大的个人信息泄露案例，从受害主体、泄露信息、影响危害等 3 个方面对案例进行分析，总结了公民个人信息泄露案件的被动收集性、群体参与性、集体博弈性、平衡对立性、连锁反应性和时间滞后性等特征。

3.1　公民个人信息泄露案例分析

随着我国以大数据、云计算、物联网为代表的信息经济迅速崛起，正在发生巨大变革的不仅是经济发展方式，还有个人生活的方方面面。便捷、高效、智能且个性化的信息服务逐渐渗透到公民生活的各个方面，与此同时，公民个人信息泄露事件的频繁发生引发了人们关于新时代下公民个人信息隐私保护的反思。

本文通过网络调研，获取了近 3 年影响较大的 27 起公民个人信息泄露案例（表 1），并对这些案例的关键要素进行了归纳（表 2）。

表 1 2020–2022 年我国公民个人信息泄露典型案例（部分）

案例序号	时间	事件
1	2022 年	总部位于美国弗吉尼亚州亨利科县的大象保险服务有限公司报告称，公司在 3 月底遭遇的一起网络安全事件可能涉及到与数百万保单客户相关的信息。
2	2022 年	中国农业银行广西崇左江州支行在崇左幼儿师范高等专科学校千余名毕业生不知情的情况下，超范围使用用户个人信息，私自批量开立Ⅱ、Ⅲ类电子账户共 12 536 户。
3	2022 年	北京市某科技公司在 2015–2019 年组建了爬虫技术团队，在未经过平台和求职者直接授权的情况下，爬取大型招聘平台求职者简历相关数据，涉及 2.1 亿余条个人信息。
4	2022 年	公民李某辉、汤某峰等人在没有取得北京冬奥组委会授权的情况下，开发“冬奥知识竞赛平台”并非法获取全国部分大中专院校在校学生个人信息共 350 余万条，同时骗取部分参与者缴纳的证书工本费 1 000 万余元。
5	2021 年	江苏省何某利用为相关单位、企业建设信息系统之机，非法获取医疗、出行、快递等行业领域的公民个人信息数 10 亿条，搭建对外提供非法查询服务的数据库，通过暗网发布广告招揽客户，出售谋取不法利益。
6	2021 年	湖北省武汉某公司工作人员徐某等人，通过李某个人编写的多款外挂程序，利用系统接口漏洞，窃取酒店、燃气、医疗健康等领域 33 个网站的后台公民个人信息数据 3 000 余万条用于债务催收等用途。
7	2021 年	安徽省吴某成立多家健康咨询公司，通过网上购买及交换有购买保健品相关记录的老年人信息共 200 余万条，再通过制定话术和夸大效果进行虚假保健品推销，共向 6 万余名老年人骗取 1 500 余万元。
8	2021 年	公民关某利用多个空壳公司与多家电信运营商签订合同并非法获取电信用户手机上网标签数据 2 亿余条，然后按照地域、行业等分类并向下游精准营销人员和电信网络诈骗犯罪人员贩卖进行牟利。
9	2021 年	福建省公安机关查明，公民谢某诱骗某电商平台店铺客服点击木马链接，窃取了 200 余家店铺买家个人信息共 1 000 余万条，后向他人层层贩卖牟利，导致个人信息数据最终流向电信网络诈骗团伙。
10	2021 年	山东省某网络科技公司从网上购买公民信息，在辽宁省阜新市石某团伙的技术支撑下，突破游戏公司验证机制，非法注册实名网络游戏账号 1.8 万余个并向未成年人出售，非法牟利 170 余万元。
11	2021 年	珠海市某艺术品策划公司通过某 App 后台维护人员汪某购买 App 运营过程中获取到的古董持有人的个人信息共 200 万余条，并以协助拍卖古董为名骗取客户服务费及托管费进行非法牟利 1.9 亿余元。同时该公司员工邝某、黄某为谋取私利，将公司非法获取的个人信息向其他电信网络诈骗团伙进行贩卖牟利。
12	2021 年	江苏省某公司非法搭建了 5 300 余个虚假网站，并冒用其他公司资质在某自媒体平台发布虚假信息，诱导免费领取男科用药、白酒、保健品等物品，并引流到公司所建虚假网站，骗取公民个人信息 110 余万条并贩卖牟利，包括网民的姓名、手机号、收货地址等。
13	2021 年	浙江省李某指使团伙成员应聘多家快递公司临聘人员，利用整理快递包裹的机会，偷拍快递面单 2 万余张，进行个人信息的汇总整理后在网上贩卖牟利。
14	2021 年	江苏省张某搭建服务器制作远程控制软件，出售给他人安装在受害人手机上，非法获取用户手机的位置、通话记录等个人信息，涉及手机 1.1 万余台。
15	2021 年	公民连某某利用 Telegram 聊天软件，通过共享和向他人购买等非法手段获取各类公民个人信息共计 200 余万条，包括学籍信息、个人简历、银行开户信息、贷款信息等，并出售获取的个人信息 3 万余条。
16	2020 年	任某某、黄某等人，通过孙某某开发了的“终端查预缴 0903”外挂软件，链接到中国移动公司网站，非法窃取中国移动公司客户的个人信息，包括客户姓名及业务订单等内容。之后，黄某将窃取到的公民个人信息交给任某某 50 561 条，任某某将获取到的信息下发给公司员工，让员工开展业务。期间，李某某伙同黄某以同样方式获取公民个人信息 40 万余条。2017 年左右，孙某某通过编写程序软件、伪造用户 ID，从“格格家购物平台”秘密爬取了 6.5 万余条信息，包括购物者的姓名、电话、住址等个人信息。
17	2020 年	2020–2021 年 2 名航空公司员工利用职务之便获取公民个人信息并出售，包括他人乘坐航班的行踪轨迹信息 1 964 条，其他公民个人信息 370 条。此外，两人还分别通过各自渠道单独获取并出售个人信息获利，2 名明星粉丝也因购买涉案信息被控有罪。
18	2020 年	姚某某、戎某在其住所通过 QQ、微信等社交平台购买和出售公民姓名、通信、通讯联系方式等公民个人信息。姚某某负责联系上家、下家，购买、出售公民个人信息，戎某负责利用购买来的公民个人信息“上粉”和出售。期间两人非法获利 2 万元以上并平分。
19	2020 年	春节前后，超过 7 000 名武汉市返乡者信息遭泄漏，微博上关于武汉市返乡人员信息被泄漏的相关话题阅读量超过 2 800 万，留言反馈者中不少是武汉市各大高校的学生。
20	2020 年	有暗网用户发布了一则交易信息，名为“5.38 亿微博用户绑定手机号数据，其中 1.72 亿有账号基本信息”，售价为 1388 美元。其中绑定手机数据包括用户手机号和 ID 及账号基本信息，包括头像、昵称、所在地、粉丝数等。
21	2020 年	山东省胶州市市民的微信群里出现市中心医院出入人员名单相关信息，涉及 6 000 多名人员的姓名、住址、身份证号码、联系方式等个人信息，造成了不良的社会影响。
22	2020 年	有媒体报道，浙江省某银行员工违规泄漏客户信息，银行被罚款 30 万，泄漏信息的人员被禁业 3 年。江苏省淮安市建设银行某员工将银行卡使用人的身份信息、电话号码、余额甚至交易记录以每条 80~100 元的价格售卖获利，涉及个人信息 5 万多条。

续表 1

案例序号	时间	事件
23	2020 年	郑州西亚斯学院近 2 万名学生信息遭到泄漏，包括姓名、身份证号、专业、宿舍门牌号等 20 余项信息，多名学生反映收到骚扰电话。河南财经政法大学、西北工业大学明德学院等高校的数千名学生信息被企业冒用，学生个人所得税 App 上有陌生公司的就职记录。
24	2020 年	圆通快递公司多名内部人员与不法分子勾连，通过有偿租用圆通快递内部员工系统账号方式盗取公民个人信息，导致 40 万条公民个人信息被泄漏后被层层倒卖，事件曝光后引起轩然大波。媒体调查发现，多家快递公司存在网上贩卖快递用户信息的现象，大量包含快递客户姓名、住址、电话的个人信息被打包出售。
25	2020 年	广西壮族自治区妇幼保健院利用工作的便利，在为新生儿办理出生证时，非法下载新生儿和产妇的个人信息并倒卖，总量达 89 904 条。
26	2020 年	2020 年 10 月 15 日，央视新闻报道，江苏泰州警方破获一起侵犯公民个人信息案，抓获犯罪嫌疑人 7 名，被售卖的公民个人信息达 800 多万条。
27	2020 年	江苏省公安机关成功侦破 3.26 特大贷款类电信网络诈骗案，网络推广团伙非法获取了 40 万条贷款申请人的个人信息，并以每条 30~50 元不等的价格出售给电信网络诈骗分子，受害人达 4 700 名，涉案金额 1.1 亿元。

表 2　公民个人信息泄露类型及典型案例

类型	案例序号	责任单位/责任人	受害主体	手段	泄露体量	泄露的个人信息类型	年份
信息泄露	1	大象保险服务有限公司	用户	泄露	数百万条数据	个人基本信息	2022
	19		武汉返乡者	泄露	超 7 000 条数据	个人基本信息、返乡信息	2020
	20	微博	用户	泄露、售卖	1.72 亿条数据	个人账号信息	2020
	21	山东胶州市中心医院	公民	泄露	超 6 000 条数据	个人基本信息、医疗信息	2020
	23	郑州西亚斯学院	高校学生	泄露、冒用	近 2 万条数据	个人基本信息	2020
信息盗取	2	中国农业银行广西崇左江州支行	高校学生	非法获取、冒用	12 536 条账号数据	个人基本信息	2022
	3	北京某科技公司	用户	非法盗取	2.1 亿余条数据	个人基本信息、求职信息	2022
	4	李某辉、汤某峰	高校学生	非法盗取	350 余万条数据	个人基本信息	2022
	5	江苏何某	公民	非法盗取	数 10 亿条数据	个人基本信息、医疗信息、出行信息	2021
	6	徐某、李某	用户	非法盗取	3 000 余万条数据	个人基本信息、债务催收信息	2021
	8	关某	用户	非法盗取、售卖	2 亿余条数据	手机上网标签数据	2021
	9	谢某	用户	非法盗取、售卖	1 000 余万条数据	个人基本信息、收货信息	2021
	12	江苏省某公司	网民	非法盗取、售卖	110 余万条数据	个人基本信息、收货信息	2021
	13	李某及其团伙	公民	非法盗取、售卖	2 万余条数据	个人基本信息、收货信息	2021
	14	张某	公民	非法盗取	手机 1.1 万余台	个人基本信息、通信信息	2021
	16	任某某、黄某等人	客户	非法盗取	40 万余数条数据	个人基本信息、通信信息	2020
	17	两名航空公司员工	客户	非法盗取、售卖	2 000 余条数据	个人基本信息、出行信息	2020
	24	圆通快递内部人员及不法分子	客户	非法盗取	40 万条数据	个人基本信息、收货信息	2020
	27	网络推广团伙	公民	非法盗取、售卖	40 万条数据	个人基本信息、贷款信息	2020
信息交易	7	吴某	老年人	非法购买	200 余万条数据	个人基本信息、购货信息	2021
	10	山东省某网络科技公司	公民	非法购买、售卖	1.8 万余个账号	个人基本信息	2021
	11	珠海市某艺术品策划公司	用户	非法购买、售卖	200 万余条数据	个人基本信息、购货信息	2021
	15	连某某	公民	非法购买、售卖	200 余万条数据	个人基本信息、学籍信息、银行开户信息、贷款信息等	2021
	18	姚某某、戎某	公民	非法购买、售卖		个人基本信息	2020
	22	浙江省的银行内部员工	客户	售卖	5 万多条数据	个人基本信息、交易信息	2020
	25	广西壮族自治区妇幼保健院员工	客户	售卖	89 904 条数据	个人基本信息、医疗信息、出生信息	2020
	26	不法分子		非法获取、售卖	800 多万条数据		2020

3.1.1　受害主体范围广泛

通过梳理可以看出，信息泄露的受害主体既有普通公民、农民工，也有高校学生，覆盖了多个平台、公司或单位的用户、客户及网民群体。这说明知识文化水平并不能够成为判断是否会发生信息泄露案件的有效标准，具有较高文化素质的高校大

学生群体依旧成为了信息泄露事件的受害者。这也从侧面反映了当前非法获取信息的技术手段发展之先进、渗透之广泛，即便是对具有一定信息保护意识、具备个人信息保护能力的人来说依旧防不胜防。一些知名企业、单位及互联网平台没有很好地遵守相应的法律法规、道德规范，没有尽到应尽的保密义务，反而在利益的驱使下做出一系列侵犯他人信息安全的行为，损害了其自身声誉，也辜负了民众的信任。

3.1.2 泄露信息类型多样

表 2 显示，自 2020 年以来，影响较大的公民个人信息泄露案例可分为信息泄露、信息盗取和信息交易 3 种类型。信息泄露是指部分服务平台、管理单位的用户/人员数据被批量泄露甚至贩卖，数据主要以个人基本信息和账号信息为主；信息盗取是指一些不法分子利用爬虫、外挂和木马病毒等技术手段，或者利用工作之便非法盗取并售卖大量个人基本信息、收货信息、通信信息等；信息交易是指一些不法分子通过非法途径购买或售卖大量的个人基本信息、购货信息等。被泄露的信息内容以个人基本信息为主，同时还包括账号信息、通讯信息、收货信息、购买信息、医疗信息、出行信息、求职信息等，基本涵盖了个人信息的全部类型。个人信息泄露案件频发、涉及的信息内容广泛，公民几乎毫无隐私可言，一切能够转化为利益的信息与数据都有受到侵犯的风险。

3.1.3 负面影响恶劣

信息泄露造成的负面影响广泛而恶劣，不法个人或集体通过非法泄露、非法盗取、非法购买和售卖等手段侵犯公民的个人信息牟利，泄露的数据体量少则上千条，多则数亿条，数据量巨大，非法获利金额不菲。这些个人信息泄露事件都产生了不良的影响，轻则通过短信电话骚扰公民的正常生活，重则通过诈骗等非法手段侵害公民的个人财产、破坏社会公平，危害了社会的和平稳定与长治久安。虽然信息泄漏的相关话题会随着重大案件的发生不时见诸报端，引发群众的广泛讨论与密切关注，但并不能从源头解决问题，也不能减轻信息泄露已造成的各种负面影响。因此，信息泄露乱象的整治刻不容缓，有必要拟定更具针对性的对策措施、实施更有效的惩治手段。

3.2 公民个人信息泄露特征分析

通过文献调研和对公民个人信息泄露典型案例的分析，本文总结归纳了公民个人信息泄露案件的六大特征。

3.2.1 被动收集性

公民参加购物、扫描健康宝、办理银行业务、购买车船飞机票、参加线上培训、发表学术论文、注册社交软件及学习软件等社会活动时，一般都会根据要求填写个人信息或被后台软件自动抓取行为数据，很多情况下基于服务“霸王条款”公民只能被动同意，因此个人信息被大量收集，信息被非对称占有，从而构成潜在危险。

3.2.2 群体参与性

如今手机已成为人们出行和办理业务的重要工具，购物支付、旅行购票、学习注册等都离不开手机，尤其是疫情期间很多公共场合要求出示健康宝或行程卡，只要公民出门参与社会活动就必须出示健康宝或行程卡，大量个人信息就会被全范围采集，呈现出了群体参与的特点。

3.2.3 集体博弈性

公民个人信息泄露有一部分是个人无意泄露的，但后果比较严重的是机构非法批量出售个人信息。而且泄密与反泄密已不仅是简单的个人泄密问题，涉及到法律制度、行业管理、技术防范、网络渗透与反渗透等多个领域，是公民、政府执法机关与出售个人信息团伙的集体博弈。

3.2.4 平衡对立性

目前个人隐私保护的痛点在于人们享受技术带来的便利的同时，也需面对技术带来的弊端。数据成为资产的现实使大多数机构愈发迫切地想要掌握更多数据，关于各种 App 要求强制授权、过度收集个人信息的话题热度不减，互联网上不法分子的阴暗操作让人防不胜防。平衡个人数据共享和隐私保护存在的对立性是重中之重，如精准购物推荐和个人行为痕迹记录。一方面，精准推荐给我们带来更多的视野，方便我们做更好的选择；另一方面我们又必须面对令人厌烦的行为定向营销。

3.2.5　连锁反应性

网络时代，信息快速传播使个人信息泄露的蝴蝶效应愈发明显。很多情况下，一不留神的一次按键授权会导致敏感信息泄露呈网状快速蔓延，引发一系列的不良反应，甚至愈演愈烈，引起轩然大波。

3.2.6　时间滞后性

很多情况下，个人信息被收集后并不会马上泄露出去，信息收集后还有信息处理、出售和利用的过程。因此，很多个人信息泄露案例存在一定的时间滞后性，这也给受害主体造成了一定的麻痹，使保密管理更加被动，不易跟踪和追溯。

4　公民个人信息泄露途径及原因

4.1　公民个人信息泄露途径

4.1.1　个人手机等智能设备成为个人信息泄露重要渠道

一是 App 等应用程序过度采集个人信息情况严重。大量 App 通过非法设置手机安装和使用权限获取用户手机通讯录、相册、地址等信息，借助精准的人工智能推荐算法，从年龄、偏好、习惯、地域、交往、饮食、运动等多角度对用户进行分析，一些 App 为保证用户真实性还需上传人脸照片进行认证，从而为用户精准画像。2021 年 5 月，国家互联网信息办公室在公众大量使用的 App 中抽取了 105 款，对这些 App 收集使用个人信息的情况进行了检测，发现了很多问题，如未经用户同意收集使用个人信息；违反必要原则，收集与其提供的服务无关的个人信息；未公开收集使用规定等，存在非法获取、超范围收集、过度索权等违规收集使用个人信息的现象。

二是微信、QQ 等即时通讯工具成为公民个人信息泄露的重灾区。有调查结果显示，很多人把注册微信需要填写的基本信息设置为真实信息，有的甚至把职务加姓名设置为用户昵称，把头像设置为私人照；有的人对用户权限设置较低，添加好友未开启验证功能，朋友圈允许陌生人查看，位置信息处于允许共享状态。微信用户均可通过以上开放信息迅速锁定个人身份，成为不法分子窃密的重要目标。

三是可穿戴设备成为泄密渠道。可穿戴设备集成了嵌入式操作系统、内置传感器、数据采集、无线自组网等技术，通过设备软件支持和信息交互、云端交互来实现强大的功能，如智能手环、谷歌眼镜、智能头盔等。可穿戴设备体型小巧，外观与普通穿戴相似，可随着人的活动而活动，利用各种传感器随时随地采集周围的各种数据，如影像、声音、气象、地理坐标、行动轨迹等信息，一旦进入个人生活区域，可轻易获得个人信息。可穿戴设备采用的无线连接和开放操作系统，能够实时连接移动通信网络、无线网络，容易遭到非法远程控制，成为个人信息泄露的隐秘通道。

4.1.2　第三方恶意技术入侵盗取公民个人信息

常见的主要是网上黑客攻击和针对具体单位和人员的信息偷窃。2022 年 5 月，大象保险服务有限公司美国总部报告称，公司在 3 月底遭遇的一起网络安全事件可能涉及到数百万份保单客户的相关信息，公司在检测到“网络上存在异常活动”之后立即展开调查，并确定入侵者可能获取了包括姓名、驾驶执照号码和出生日期在内的信息，给用户的生活秩序造成重大风险隐患，产生了很大的负面影响。

4.1.3　数据采集机构非法出售个人信息

大数据时代，公民个人信息的商业价值被充分挖掘，拥有个人信息的机构在信息时代就是拥有巨额财富，也是境外机构的重点收集目标。在利益驱动下个人信息容易被不法分子售卖，如 2018 年“数据堂”特大侵权公民个人信息案。据公安部门统计，“数据堂”一个月内日均传输个人信息 1.3 亿条，规模之大令人触目惊心。再如 2021 年轰动全球的“滴滴”事件，“滴滴出行”App 存在严重违法违规采集个人信息问题，为避免扩大风险，国家互联网信息办公室通知网络应用商店下架“滴滴出行”App，停止新用户注册。

4.1.4　政府机关及公共服务部门采集和公示个人信息

随着“互联网+”及无纸化办公的快速推进落地，各项数据信息化建设也向着“云平台+”建设推进，各级政府、机关和公共服务部门在采集数据时，会要求公民提供超过本部门需求的信息，存在

过度采集和随意采集问题。如公民的邮箱信息、身份证号、家庭住址、家庭成员信息、手机号等信息被采集后，可能会遭到泄露；还有一些政府、机关单位及公共服务部门对公民信息进行公示，被公示的个人信息也存在泄露的风险。

4.2 公民个人信息泄露原因

4.2.1 国家信息安全法律体系不完善导致不法分子有漏洞可钻

一是国家个人信息保护的法律体系不够完善。我国从宪法、各类法律、法规、规章到所签订的国际条约都对个人信息保护进行了规定。但相关规定侧重于理论，操作性不强，相关条文零散分布，缺乏统一性和体系性，个人信息的概念不清、界限模糊，个人信息保障范围有限，信息侵犯主体范围模糊，侵犯行为判断易出现偏差。如个人信息保护的法律大多是针对安全问题发生后的惩处，对个人的行为规范却并不多，很难从根本上对个人信息安全问题进行有效预防；《中华人民共和国网络安全法》《信息安全技术个人信息安全规范》等法律规范对个人信息进行了定义，但判定标准仍然不够明确，执法部门难以参照相关内容判断出遭窃取、泄露的信息是否为个人信息，容易让犯罪分子钻法律的空子，得不到应有的法律制裁。

二是国家执法力度不强。一些组织或个人出于谋取非法利益等目的，违反职业道德和保密义务，以窃取、收买、非法提供等方式大肆收集、存储、利用、泄露公民个人信息，特别是一些政府机关或公共服务部门在履行公务或提供服务时获取的公民个人信息被非法泄露的情况时有发生。然而在司法实践中，司法机关对侵犯公民个人信息的案件没有足够重视，没有开展强有力的司法审判和执行。在现行相关法律中，对泄露、窃取个人信息的相关违法行为，通常都是罚款为主，不法分子很少会承担刑事责任。售卖个人信息的收益显然要远高于违法成本，致使出售或非法提供个人信息的活动越来越猖獗。

4.2.2 保密意识不强使政府机关及公共服务部门无意泄露公民个人信息

政府信息公开是促进政府职能转变的有力战略，然而在公民个人信息保密方面，一些政府机关及公共服务部门存在行政部门职能缺失的问题。一是在处理公民个人信息的各个阶段中，相关工作人员缺少对公民信息保密的意识，注意力主要放在完成相应的工作上，造成信息泄露的现象。如一些公共服务部门工作人员对个人信息的保密性认识不到位，展示了不该展示的内容，导致公民个人信息泄露。二是政府机关及公共服务部门缺乏对工作人员的管理和监督，导致相关工作人员的信息安全意识不强。有些工作人员对公民信息采集及公开的范围、内容缺乏清晰的认识，容易过度收集公民个人信息，跨越收集原则的底线，使公民成为“透明人”。甚至有些工作人员在行使权力的过程中不遵守相关制度和规定或不按程序操作，增加了公民隐私泄露的风险。

4.2.3 趋利性使商业机构非法兜售个人信息

个人信息商品化使售卖个人信息成为不法分子牟利的恶劣手段。一方面是不法分子形成黑色产业链，非法采集、加工、售卖、购买、转售并非法利用个人信息。另一方面是大数据公司通过利用高新科技手段在未经允许的情况下非法追踪抓取个人信息，通过对零散细碎个人信息拼接组合进行数据挖掘分析，暴露公民个人信息。

4.2.4 斗争性使境外机构不择手段获取个人信息

一是境外情报机构渗透，策反窃密活动无孔不入。这些机构紧盯核心重要涉密人员，不择手段胁迫策反我国在境外人员，通过多种渠道结识、攀拉我国涉密人员，非法窃取国家机密情报。二是境外情报机构不断加大网络窃密攻击力度，目标直指核心要害部门。攻击密集，指向明确，紧盯我国大事要事，高端智库、知名学者的计算机成为境外机构攻击重点。三是境外反华势力文化入侵。美国利用网络空间霸权进行政治引导及价值观输出，美国文化产品所宣扬的拜金主义、享乐主义和利己主义等价值理念都通过网络渗透影响青少年价值观，一些人追求所谓的“民主和自由”，向往奢靡享乐的生活，无视保密规定铤而走险。

4.2.5 技术落后导致信息安全监管能力不足

一是信息领域核心技术落后。软件方面，大多

数计算机采用 Windows 系列操作系统，后台核心代码非我国控制，容易在未经允许的情况下保存浏览器数据，并私自上传数据到境外的服务器上，给我国公民个人信息安全带来巨大风险。硬件方面，我国芯片技术被“卡脖子”，智能设备和信息采集设备核心芯片容易被远程操控留“暗门”，难以杜绝植入芯片窃取数据等安全问题，使用这些设备的个人信息存在安全隐患。二是信息监管防护能力不高。个人信息的泄露通常需要经过采集、整理、发布或出售几个阶段。如一些软件会利用 Cookie 文件对上网人员的浏览记录、用户名、密码和 IP 地址等详细信息进行记录，然后对数据进行标引识别后处理销售。这些流程记录行为缺乏有效的信息安全监控管理技术，任何一个环节若能够得到有效监管都可以大大降低信息泄露的风险。

4.2.6　公民隐私保护教育不力

一是公民个人信息保密意识不强。我国对隐私保护教育重视不够，个人隐私防范风险意识不强，不了解隐私泄露途径，用网随意不设防；个别人虚荣心作祟，难抵金钱美色诱惑，为在短期内获得极大利益回报不惜铤而走险。

二是个人信息安全法律教育不足。《中华人民共和国个人信息保护法》2021 年才颁布实施，公民关于个人信息保护的法律知识欠缺，个人信息安全受到侵犯时难以想到通过法律手段保护个人信息安全。

5　公民个人信息安全保密对策

5.1　构建完善的个人信息保护法律体系加强个人信息司法保护

一是要完善国家关于个人信息保护的法律体系。尽管近年我国集中颁布并实施了《中华人民共和国个人信息保护法》、《中华人民共和国数据安全法》和《中华人民共和国网络安全法》等有关个人信息保护的法律。但这些法律刚刚实施，还存在一些没有特别明确的问题，相关部门应在后续的法律实施过程中对法律条文中的一些细节进行规范明确的说明，避免不法分子钻法律漏洞，导致公民信息泄露带来不必要的损失。

二是要加大处罚力度，提高违法成本。《中华人民共和国刑法》第二百五十三条规定：违反国家有关规定，向他人出售或者提供公民个人信息，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。《中华人民共和国消费者权益保护法》和《中华人民共和国网络安全法》则基本以现金罚款为重。上述法律法规规定的刑期和罚款金额，相对于愈演愈烈的侵犯公民信息犯罪行为相比，明显过轻，违法犯罪成本过低。因此，立法应加大侵犯公民个人信息行为的处罚力度，特别是如侵犯公安人员、军人、儿童等特殊群体个人信息的还应从重处罚。

5.2　加强行政监管

政府机关及公共服务部门要提高对公民个人信息的保护意识，充分发挥地方行政保护的力量，强化地方行政机关对公民信息保护的监管责任，成立公民个人信息保护机构，加强信息监督，严格执法，即时有效制裁各种个人信息侵权行为，追究违法企业主体责任。必要时应采取联合执法模式，全方位打击治理侵犯个人信息的违法行为，建立完善的事先责任制和事后问责追究制，避免因政府机关及公共服务部门过度采集个人信息而导致公民个人信息泄露。同时，政府机关及公共服务部门应加强对工作人员的管理与监督，对他们进行公民个人信息保密方面的培训，建立和完善奖惩机制，加大内部约束力，从制度上、思想上、行为上对从业人员进行约束，实现对公民隐私权利的保障。

5.3　加强经营者主体责任，平衡公民权益保护和数字经济发展

互联网及大数据公司是个人信息汇聚的重要地点，信息流入流出都会经过这些公司的数据处理环节。一是明确规定经营者在信息收集环节的责任和义务，严格要求运营者不得收集与提供与服务无关的信息，必须依照法律法规的规定和用户的约定处理保存信息，一旦在此过程中出现数据泄露事件，严厉追究经营者责任。二是应对运营者收集到的与所提供服务相关的公民信息进行使用记录，确

保这些信息仅应用于经营过程而不是进行非法贩卖，并且要组织相关部门定期对其信息使用记录进行审计。三是进行行业治理，制定行业守则，通过“净网”行动整顿行业乱象，充分尊重公民个人意愿，删除如“最终解释全归网站所有”等霸王条款，严格保障公民个人权益。四是在充分保护个人信息安全的同时，通过技术措施平衡数字经济发展。

5.4 增强忧患意识和敌情观念，加强防间反窃密能力

正确把握国际国内形势发展变化，要充分意识到信息时代信息传播和获取的便捷性。互联网已成为政治渗透的新工具和意识形态斗争的新战场，我们必须强化互联网信息泄露的风险意识，尽量避免通过互联网传输涉密信息，一定需要传输的应尽量采取光盘刻录的形式。此外，还应当加强泄密风险预判预警，增强忧患意识和敌情观念，克服麻痹大意思想，时刻保持警惕和清醒头脑，提升信息化条件下防范化解重大失泄密风险的能力水平，采取有针对性的综合措施，下好先手棋，打好主动仗。

5.5 发展自主信息安全技术，提升个人信息泄露技术对抗能力

目前个人信息主要通过网络传播。如果采集、存储和传播个人信息的网络不能完全自主可控，那么这个网络平台则存在巨大隐患。若想从根本上摆脱对国外基础软硬件的依赖，避免因网络传播而导致信息泄露，应采取以下措施。一是大力推进信息产业基础技术自主可控发展，从基础软硬件源头防范暗门风险。基础软硬件包括支撑系统安全运行的硬件、固件、操作系统等。二是大力推进信息产业中间平台和应用技术发展，在信息采集传输环节加强个人信息安全防范。中间平台主要是指云计算平台、大数据平台、并行计算平台等。应用层主要指各种办公、数据处理和功能应用的运行程序。这些软件最易被植入后门，遭受病毒和黑客攻击，这也是个人信息泄露的重要原因。三是大力发展个人信息数据处理技术，提升信息传播检测预警能力。加强如文件加密技术、身份认证技术、个人信息录入提醒技术等个人信息采集技术的研究，增强源头性保护；加强如社交网络匿名保护技术、数据发布匿名保护技术，数据溯源技术等个人信息处理技术的研究，推进过程性保护；加强如入侵检测技术、防火墙技术、杀毒软件等防护技术的研究，提升信息安全防御；加强个人信息监测预警技术的研究，加强风险预判处置能力。

5.6 加强公民隐私保护教育和管理，提升个人信息安全防范能力

加大个人信息保护宣传教育力度，提升隐私保护法治教育的针对性和有效性。通过进行个人信息保护宣传教育，提升个人信息防护意识。即时更新教育内容，让公民充分了解网络信息发布的漏洞和窃取信息的途径；引导公民重视对日常生活信息的管理，如拒绝向来历不明或存在风险的组织或个人提供个人信息，不在“朋友圈”、微博等社交网络发布可能暴露隐私的照片或文字，保管好银行凭据、快递单据、车票等包含个人信息的文件，丢弃前可采取对关键信息进行涂抹或粉碎等处理。总之，不断增强公民的保密意识，加强个人信息泄露防御能力。

6 结语

如今，互联网已融入我们的生活，网络购物、交通出行、线上交易等应用程序便利了我们的生活，但同时也会更多地收集公民的个人信息，使个人信息安全面临更大的威胁。当前，我国在法律体系、政府监管、保密意识、技术服务等方面对个人信息的保护尚有明显不足，需紧跟时代变革的节奏和步伐，加大对个人信息的保护力度。首先，政府机关应树立责任意识，加强对工作人员保密知识的教育培训，完善相关法律体系，加大行政监管和惩罚力度；第二，公民个人要增强防范意识和责任意识，重视对日常生活信息的管理，强化互联网信息泄露的风险意识，加强民族责任意识，以避免被利益驱使出卖他人信息；第三，发展自主信息安全技术，增强防泄露技术研究能力，提升个人信息加密技术水平。综上所述，我国应建立健全的信息保护治理体系，构建产业协同的安全保障网络，进一步明确公民个人信息使用规则[38]，真正实现对公民个人信息的保护，促进信息社会建设。

【参考文献】

[1] 姚雨蒙. 国内外个人信息保护规制差异与实践探索[J]. 河北公安警察职业学院学报，2022，22(2)：52-55.

[2] 邵晶晶，韩晓峰. 国内外数据安全治理现状综述[J]. 信息安全研究，2021，7(10)：922-932.

[3] 刘　享. 大数据背景下个人信息安全法律问题研究[J]. 法制博览，2021(13)：36-37.

[4] 吴佳怡. 大数据时代个人信息行政法保护研究[D]. 贵阳：贵州财经大学，2021.

[5] 钱桂鑫. 大数据时代视阈下民法个人信息保护的策略[J]. 法制博览，2021(31)：41-42.

[6] 马宝林. 数字信息环境下个人信息保护的困境及民事纠纷解决的相关思考[J]. 法制博览，2021(18)：40-41.

[7] 杜　鹃. 对公民个人信息刑法保护问题的法律完善[J]. 法制与社会，2021(8)：14-15.

[8] 张伟一. 网络环境下个人信息保护的行政监管[D]. 兰州：甘肃政法大学，2021.

[9] 王光祖. APP 收集个人信息的行政法规制[D]. 北京：中国人民公安大学，2021.

[10] 范文英，赵　华，杨　菲，等. 电子支付中的个人信息保护问题研究[J]. 法制博览，2021(35)：18-20.

[11] 李宗亿. 论个人生物识别信息的隐私权保护路径[D]. 上海：上海师范大学，2021.

[12] 刘坤峰，郝国芬，刘欣慧，等. 疫情防控背景下个人信息安全问题与对策研究[J]. 法制与社会，2021(6)：13-14.

[13] 李　晗. 大数据时代网上银行的信息安全保障义务研究[J]. 法学杂志，2021，42(4)：53-66.

[14] 王晓鹏. 电商背景下个人信息泄露情况及对策研究[J]. 上海商业，2021(10)：38-39.

[15] 王亚彤. 快递服务中消费者个人信息保护研究[D]. 石家庄：河北经贸大学，2021.

[16] 肖　通. 数字化转型背景下民航旅客信息保护的现状与对策[J]. 民航管理，2021(6)：39-42.

[17] 何金海. 论在线旅游经营服务中的旅游者个人信息保护[J]. 太原学院学报：社会科学版，2021，22(5)：35-43.

[18] 刘　鹏，李德伟. 大数据趋势下的搜索引擎用户信息安全探讨[J]. 网络安全技术与应用，2021(7)：69-71.

[19] 李宁薇. 内幕交易者的信息泄露行为分析[D]. 长春：东北师范大学，2021.

[20] 戴文奎，李学成. 个人隐私泄露的途径与防范研究[J]. 电脑知识与技术，2021，17(25)：57-59.

[21] 金元浦. 大数据时代个人隐私数据泄露的调研与分析报告[J]. 清华大学学报：哲学社会科学版，2021，36(1)：191-201，206.

[22] 韩　缨，杨观帝. 我国公民个人信息保护的挑战与对策[J]. 法制博览，2021(10)：45-47.

[23] 张智浩. 公民个人信息保护现实困境与突破[J]. 洛阳理工学院学报：社会科学版，2021，36(1)：54-62.

[24] 王　灏. 公民个人信息安全防控体系研究[J]. 西南民族大学学报：人文社会科学版，2020，41(12)：82-87.

[25] 郭雪慧. 人工智能时代的个人信息安全挑战与应对[J]. 浙江大学学报：人文社会科学版，2021，51(5)：157-169.

[26] 马百喜. 大数据分析的隐私信息保护方法研究[J]. 网络安全技术与应用，2021(1)：73-75.

[27] 黄薪宇. 个人信息泄露检测模型的对抗攻击研究[D]. 北京：北京邮电大学，2021.

[28] 曲滨鹏，缪　佳，朱丽娜，等. 基于计算机技术对涉密信息的保护探讨[J]. 电脑知识与技术，2021，17(27)：57-58.

[29] 李婧欣. 面向边缘计算的任务卸载隐私保护研究[D]. 武汉：武汉大学，2021.

[30] 张毅刚. 基于数据流的 Android 应用信息泄露检测平台的设计与实现[D]. 北京：北京邮电大学，2021.

[31] 王彩玲. 位置大数据中基于隐私保护的加密技术研究[J]. 信息系统工程，2020(7)：76-78.

[32] 熊　斌. 大数据时代个人隐私保护的路径重构[J]. 现代企业，2020(10)：78-79.

[33] 刘　錞. 基于矩阵变换的大数据隐私保护关键技术研究[D]. 郑州：战略支援部队信息工程大学，2020.

[34] 闫坤如. 大数据的共享-隐私悖论探析[J]. 大连理工大学学报：社会科学版，2020，41(5)：15-20.

[35] 张志悦. 大数据发展与隐私保护问题研究[J]. 内蒙古科技与经济，2020(9)：71-72.

[36] 杨　扬. 大数据语境下个人信息隐私安全的伦理研究[D]. 济南：山东师范大学，2020.

[37] 国家市场监督管理总局，国家标准化管理委员会. 信息安全技术个人信息安全规范：GB/T 35273-2020[S]. 北京：中国标准出版社，2020.

[38] 赵莹雪. 公民个人信息保护治理体系需完善[N]. 北京日报，2020-12-02(14).

[收稿日期：2022-05-07]

[本文编辑：黄思敏]