



关于侵犯公民个人信息罪 法律法规汇编

宁波市律师协会互联网与数字化专业委员会

二〇二五年十二月

目录

一、法律

- （一）中华人民共和国刑法（2023 年修正）
- （二）中华人民共和国个人信息保护法
- （三）中华人民共和国网络安全法

二、司法解释、司法文件

- （一）最高人民法院、最高人民检察院《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》【法释〔2017〕10 号】
- （二）最高人民检察院《检察机关办理侵犯公民个人信息案件指引》【高检发侦监字〔2018〕13 号】
- （三）最高人民法院、最高人民检察院、公安部《关于办理信息网络犯罪案件适用刑事诉讼程序若干问题的意见》【法发〔2022〕23 号】
- （四）最高人民法院 最高人民检察院 公安部《关于依法惩治网络暴力违法犯罪的指导意见》【法发〔2023〕14 号】
- （五）最高人民法院、最高人民检察院、公安部《关于办理电信网络诈骗等刑事案件适用法律若干问题的意见（二）》【法发〔2021〕22 号】
- （六）最高人民法院、最高人民检察院、公安部《办理跨境赌博犯罪案件若干问题的意见》【公通字〔2020〕14 号】
- （七）最高人民法院《人民法院落实〈保护司法人员依法履行法定职责规定〉的实施办法》【法发〔2017〕4 号】
- （八）最高人民法院、最高人民检察院、公安部《关于办理医保骗保刑事案件若干问题的指导意见》【法发〔2024〕6 号】

三、规范性文件

- （一）公安部、北京市网络行业协会《互联网个人信息安全保护指南》

法律

（一）中华人民共和国刑法（2023 年修正）

第二百五十三条之一【侵犯公民个人信息罪】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。

违反国家有关规定，将在履行职责或者提供服务过程中获得的公民个人信息，出售或者提供给他人的，依照前款的规定从重处罚。

窃取或者以其他方法非法获取公民个人信息的，依照第一款的规定处罚。

单位犯前三款罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，依照各该款的规定处罚。

（二）中华人民共和国个人信息保护法（2021.08.20 发布 2021.11.01 实施）

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。

（三）中华人民共和国网络安全法（2016.11.07 发布 2017.06.01 实施）

第二十二条第三款 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。

【备注】本篇法规将被《全国人民代表大会常务委员会关于修改<中华人民共和国网络安全法>的决定》修订，2025 年 10 月 28 日发布；2026 年 1 月 1 日实施。

司法解释、司法文件

（一）最高人民法院、最高人民检察院《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》【法释（2017）10号】（2017.05.08 发布 2017.06.01 实施）

为依法惩治侵犯公民个人信息犯罪活动，保护公民个人信息安全和合法权益，根据《中华人民共和国刑法》《中华人民共和国刑事诉讼法》的有关规定，现就办理此类刑事案件适用法律的若干问题解释如下：

第一条刑法第二百五十三条之一规定的“公民个人信息”，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特定自然人身份或者反映特定自然人活动情况的各种信息，包括姓名、身份证件号码、通信通讯联系方式、住址、账号密码、财产状况、行踪轨迹等。

第二条 违反**法律、行政法规、部门规章**有关公民个人信息保护的规定的，应当认定为刑法第二百五十三条之一规定的“**违反国家有关规定**”。

第三条 向特定人提供公民个人信息，以及通过信息网络或者其他途径发布公民个人信息的，应当认定为刑法第二百五十三条之一规定的“提供公民个人信息”。

未经被收集者同意，将合法收集的公民个人信息向他人提供的，属于刑法第二百五十三条之一规定的“提供公民个人信息”，**但是经过处理无法识别特定个人且不能复原的除外**。

第四条 违反国家有关规定，**通过购买、收受、交换等方式获取公民个人信息，或者在履行职责、提供服务过程中收集公民个人信息的**，属于刑法第二百五十三条之一第三款规定的“以其他方法非法获取公民个人信息”。

第五条**非法获取、出售或者提供公民个人信息，具有下列情形之一的，应当认定为刑法第二百五十三条之一规定的“情节严重”：**

- （一）出售或者提供行踪轨迹信息，被他人用于犯罪的；
- （二）知道或者应当知道他人利用公民个人信息实施犯罪，向其出售或者提供的；
- （三）非法获取、出售或者提供行踪轨迹信息、通信内容、征信信息、财产信息五十条以上的；
- （四）非法获取、出售或者提供住宿信息、通信记录、健康生理信息、交易信息等其他可能影响人身、财产安全的公民个人信息五百条以上的；
- （五）非法获取、出售或者提供第三项、第四项规定以外的公民个人信息五千条以上的；
- （六）数量未达到第三项至第五项规定标准，但是按相应比例合计达到有关数量标准的；
- （七）违法所得五千元以上的；

(八)将在履行职责或者提供服务过程中获得的公民个人信息出售或者提供给他人，数量或者数额达到第三项至第七项规定标准一半以上的；

(九)曾因侵犯公民个人信息受过刑事处罚或者二年内受过行政处罚，又非法获取、出售或者提供公民个人信息的；

(十)其他情节严重的情形。

实施前款规定的行为，具有下列情形之一的，应当认定为刑法第二百五十三条之一第一款规定的“情节特别严重”：

(一)造成被害人死亡、重伤、精神失常或者被绑架等严重后果的；

(二)造成重大经济损失或者恶劣社会影响的；

(三)数量或者数额达到前款第三项至第八项规定标准十倍以上的；

(四)其他情节特别严重的情形。

第六条为合法经营活动而非法购买、收受本解释第五条第一款第三项、第四项规定以外的公民个人信息，具有下列情形之一的，应当认定为刑法第二百五十三条之一规定的“情节严重”：

(一)利用非法购买、收受的公民个人信息获利五万元以上的；

(二)曾因侵犯公民个人信息受过刑事处罚或者二年内受过行政处罚，又非法购买、收受公民个人信息的；

(三)其他情节严重的情形。

实施前款规定的行为，将购买、收受的公民个人信息非法出售或者提供的，定罪量刑标准适用本解释第五条的规定。

第七条 单位犯刑法第二百五十三条之一规定之罪的，依照本解释规定的相应自然人犯罪的定罪量刑标准，对直接负责的主管人员和其他直接责任人员定罪处罚，并对单位判处罚金。

第八条 设立用于实施非法获取、出售或者提供公民个人信息违法犯罪活动的网站、通讯群组，情节严重的，应当依照刑法第二百八十七条之一的规定，以非法利用信息网络罪定罪处罚；同时构成侵犯公民个人信息罪的，依照侵犯公民个人信息罪定罪处罚。

第九条 网络服务提供者拒不履行法律、行政法规规定的信息网络安全管理义务，经监管部门责令采取改正措施而拒不改正，致使用户的公民个人信息泄露，造成严重后果的，应当依照刑法第二百八十六条之一的规定，以拒不履行信息网络安全管理义务罪定罪处罚。

第十条 实施侵犯公民个人信息犯罪，不属于“情节特别严重”，行为人系初犯，全部退赃，并确有悔罪表现的，可以认定为情节轻微，不起诉或者免于刑事处罚；确有必要判处刑罚的，应当从宽处罚。

第十一条 非法获取公民个人信息后又出售或者提供的，公民个人信息的条数不重复计算。

向不同单位或者个人分别出售、提供同一公民个人信息的，公民个人信息的条数累计计算。

对批量公民个人信息的条数，根据查获的数量直接认定，但是有证据证明信息不真实或者重复的除外。

第十二条 对于侵犯公民个人信息犯罪，应当综合考虑犯罪的危害程度、犯罪的违法所得数额以及被告人的前科情况、认罪悔罪态度等，依法判处罚金。**罚金数额一般在违法所得的一倍以上五倍以下。**

第十三条 本解释自 2017 年 6 月 1 日起施行。

（二）最高人民法院《检察机关办理侵犯公民个人信息案件指引》【高检发侦监字（2018）13 号】（2018.11.09 发布，2018.11.09 实施）

根据《中华人民共和国刑法》第二百五十三条之一的规定，侵犯公民个人信息罪是指违反国家有关规定，向他人出售、提供公民个人信息，或者通过窃取等方法非法获取公民个人信息，情节严重的行为。结合《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》（法释〔2017〕10 号）（以下简称《解释》），**办理侵犯公民个人信息案件，应当特别注意以下问题：一是对“公民个人信息”的审查认定；二是对“违反国家有关规定”的审查认定；三是对“非法获取”的审查认定；四是对“情节严重”和“情节特别严重”的审查认定；五是对关联犯罪的审查认定。**

一、审查证据的基本要求

（一）审查逮捕

1. 有证据证明发生了侵犯公民个人信息犯罪事实

（1）证明侵犯公民个人信息案件发生

主要证据包括：报案登记、受案登记、立案决定书、破案经过、证人证言、被害人陈述、犯罪嫌疑人供述和辩解以及证人、被害人提供的短信、微信或 QQ 截图等电子数据。

（2）证明被侵犯对象系公民个人信息

主要证据包括：扣押物品清单、勘验检查笔录、电子数据、司法鉴定意见及公民信息查询结果说明、被害人陈述、被害人提供的原始信息资料 and 对比资料等。

2. 有证据证明侵犯公民个人信息行为是犯罪嫌疑人实施的

（1）证明违反国家有关规定的证据：犯罪嫌疑人关于所从事的职业的供述、其所在公司的工商注册资料、公司出具的犯罪嫌疑人职责范围说明、劳动合同、保密协议及公司领导、同事关于犯罪嫌疑人职责范围的证言等。

（2）证明出售、提供行为的证据：远程勘验笔录及 QQ、微信等即时通讯工具聊天记录、论坛、贴吧、电子邮件、手机短信记录等电子数据，证明犯罪嫌疑人通过上述途径向他人出售、提供、交换公民个人信息的情况。公民个人信息贩卖者、提供者、担保交易人及购买者、收受者的证言或供述，相关银行账户明细、第三方支付平台账户明细，证明出售公民个人信息违法所得情况。此外，如果犯罪嫌疑人系通过信息网络发布方式提供公民个人信息，证明该行为的证据还包括远程

勘验笔录、扣押笔录、扣押物品清单、对手机、电脑存储介质、云盘、FTP 等的司法鉴定意见等。

（3）证明犯罪嫌疑人或公民个人信息购买者、收受者控制涉案信息的证据：搜查笔录、扣押笔录、扣押物品清单，对手机、电脑存储介质等的司法鉴定意见等，证实储存有公民个人信息的电脑、手机、U 盘或者移动硬盘、云盘、FTP 等介质与犯罪嫌疑人或公民个人信息购买者、收受者的关系。犯罪嫌疑人供述、辨认笔录及证人证言等，证实犯罪嫌疑人或公民个人信息购买者、收受者所有或实际控制、使用涉案存储介质。

（4）证明涉案公民个人信息真实性的证据：被害人陈述、被害人提供的原始信息资料、公安机关或相关单位出具的涉案公民个人信息与权威数据库内信息同一性的比对说明。针对批量的涉案公民个人信息的真实性问题，根据《解释》精神，可以根据查获的数量直接认定，但有证据证明信息不真实或重复的除外。

（5）证明违反国家规定，通过窃取、购买、收受、交换等方式非法获取公民个人信息的证据：主要证据与上述以出售、提供方式侵犯公民个人信息行为的证据基本相同。针对窃取的方式如通过技术手段非法获取公民个人信息的行为，需证明犯罪嫌疑人实施上述行为，除被害人陈述、犯罪嫌疑人供述和辩解外，还包括侦查机关从被害公司数据库中发现入侵电脑 IP 地址情况、从犯罪嫌疑人电脑中提取的侵入被害公司数据的痕迹等现场勘验检查笔录，以及涉案程序（木马）的司法鉴定意见等。

3. 有证据证明犯罪嫌疑人具有侵犯公民个人信息的主观故意

（1）证明犯罪嫌疑人明知没有获取、提供公民个人信息的法律依据或资格，主要证据包括：犯罪嫌疑人的身份证明、犯罪嫌疑人关于所从事职业的供述、其所在公司的工商资料和营业范围、公司关于犯罪嫌疑人的职责范围说明、公司主要负责人的证人证言等。

（2）证明犯罪嫌疑人积极实施窃取、出售、提供、购买、交换、收受公民个人信息的行为，主要证据除了证人证言、犯罪嫌疑人供述和辩解外，还包括远程勘验笔录、手机短信记录、即时通讯工具聊天记录、电子数据司法鉴定意见、银行账户明细、第三方支付平台账户明细等。

4. 有证据证明“情节严重”或“情节特别严重”

（1）公民个人信息购买者或收受者的证言或供述。

（2）公民个人信息购买、收受公司工作人员利用公民个人信息进行电话或短信推销、商务调查等经营性活动后出具的证言或供述。

（3）公民个人信息购买者或者收受者利用所获信息从事违法犯罪活动后出具的证言或供述。

（4）远程勘验笔录、电子数据司法鉴定意见书、最高人民检察院或公安部指定的机构对电子数据涉及的专门性问题出具的报告、公民个人信息资料等。证明犯罪嫌疑人通过即时通讯工具、电子邮箱、论坛、贴吧、手机等向他人出售、提供、购买、交换、收受公民个人信息的情况。

（5）银行账户明细、第三方支付平台账户明细。

（6）死亡证明、伤情鉴定意见、医院诊断记录、经济损失鉴定意见、相关案件起诉书、判决书等。

（二）审查起诉

除审查逮捕阶段证据审查基本要求之外，对侵犯公民个人信息案件的审查起诉工作还应坚持“犯罪事实清楚，证据确实、充分”的标准，保证定罪量刑的事实都有证据证明；据以定案的证据均经法定程序查证属实；综合全案证据，对所认定的事实已排除合理怀疑。

1. 有确实充分的证据证明发生了侵犯公民个人信息犯罪事实。该证据与审查逮捕的证据类型相同。

2. 有确实充分的证据证明侵犯公民个人信息行为是犯罪嫌疑人实施的

（1）对于证明犯罪行为是犯罪嫌疑人实施的证据审查，需要结合《解释》精神，准确把握对“违反国家有关规定”“出售、提供行为”“窃取或以其他方式”的认定。

（2）对证明违反国家有关规定的证据审查，需要明确国家有关规定的具体内容，违反法律、行政法规、部门规章有关公民个人信息保护规定的，应当认定为刑法第二百五十三条之一规定的“违反国家有关规定”。

（3）对证明出售、提供行为的证据审查，应当明确“出售、提供”包括在履职或提供服务的过程中将合法持有的公民个人信息出售或者提供给他人的行为：向特定人提供、通过信息网络或者其他途径发布公民个人信息、未经被收集者同意，将合法收集的公民个人信息（经过处理无法识别特定个人且不能复原的除外）向他人提供的，均属于刑法第二百五十三条之一规定的“提供公民个人信息”。应当全面审查犯罪嫌疑人所出售提供公民个人信息的来源、途经与去向，对相关供述、物证、书证、证人证言、被害人陈述、电子数据等证据种类进行综合审查，针对使用信息网络进行犯罪活动的，需要结合专业知识，根据证明该行为的远程勘验笔录、扣押笔录、扣押物品清单、电子存储介质、网络存储介质等的司法鉴定意见进行审查。

（4）对证明通过窃取或以其他方式非法获取公民个人信息等方式非法获取公民个人信息的证据审查，应当明确“以其他方式获取公民个人信息”包括购买、收受、交换等方式获取公民个人信息，或者在履行职责、提供服务过程中收集公民个人信息的行为。

针对窃取行为，如通过信息网络窃取公民个人信息，则应当结合犯罪嫌疑人供述、证人证言、被害人陈述，着重审查证明犯罪嫌疑人侵入信息网络、数据库时的IP地址、MAC地址、侵入工具、侵入痕迹等内容的现场勘验检查笔录以及涉案程序（木马）的司法鉴定意见等。

针对购买、收受、交换行为，应当全面审查购买、收受、交换公民个人信息的来源、途经、去向，结合犯罪嫌疑人供述和辩解、辨认笔录、证人证言等证据，对搜查笔录、扣押笔录、扣押物品清单、涉案电子存储介质等司法鉴定意见进行审查，明确上述证据同犯罪嫌疑人或公民个人信息购买、收受、交换者之间的关系。针对履行职责、提供服务过程中收集公民个人信息的行为，应当审查证明犯罪嫌疑人所从事职业及其所负职责的证据，结合法律、行政法规、部门规章等国家有关公民个人信息保护的规定，明确犯罪嫌疑人的行为属于违反国家有关规定，以其他方式非法获取公民个人信息的行为。

（5）对证明涉案公民个人信息真实性证据的审查，应当着重审查被害人陈述、被害人提供的原始信息资料、公安机关或其他相关单位出具的涉案公民个人信息与权威数据库内信息同一性的对比说明。对批量的涉案公民个人信息的真实性问题，根据《解释》精神，可以根据查获的数量直接认定，但有证据证明信息不真实或重复的除外。

3. 有确实充分的证据证明犯罪嫌疑人具有侵犯公民个人信息的主观故意

(1) 对证明犯罪嫌疑人主观故意的证据审查，应当综合审查犯罪嫌疑人的身份证明、犯罪嫌疑人关于所从事职业的供述、其所在公司的工商资料和营业范围、公司关于犯罪嫌疑人的职责范围说明、公司主要负责人的证人证言等，结合国家公民个人信息保护的相关规定，夯实犯罪嫌疑人在实施犯罪时的主观明知。

(2) 对证明犯罪嫌疑人积极实施窃取或者以其他方法非法获取公民个人信息行为的证据审查，应当结合犯罪嫌疑人供述、证人证言，着重审查远程勘验笔录、手机短信记录、即时通讯工具聊天记录、电子数据司法鉴定意见、银行账户明细、第三方支付平台账户明细等，明确犯罪嫌疑人在实施犯罪时的积极作为。

4. 有确实充分的证据证明“情节严重”或“情节特别严重”。该证据与审查逮捕的证据类型相同。

二、需要特别注意的问题

在侵犯公民个人信息案件审查逮捕、审查起诉中，要根据相关法律、司法解释等规定，结合在案证据，重点注意以下问题：

(一) 对“公民个人信息”的审查认定

根据《解释》的规定，公民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特定自然人身份或者反映特定自然人活动情况的各种信息，包括姓名、身份证件号码、通信通讯联系方式、住址、账号密码、财产状况、行踪轨迹等。**经过处理无法识别特定自然人且不能复原的信息，虽然也可能反映自然人活动情况，但与特定自然人无直接关联，不属于公民个人信息的范畴。**对于企业工商登记等信息中所包含的手机、电话号码等信息，应当明确该号码的用途。**对由公司购买、使用的手机、电话号码等信息，不属于个人信息的范畴，**从而严格区分“手机、电话号码等由公司购买，归公司使用”与“公司经办人在工商登记等活动中登记个人电话、手机号码”两种不同情形。

(二) 对“违反国家有关规定”的审查认定

《中华人民共和国刑法修正案（九）》将原第二百五十三条之一的“违反国家规定”修改为“违反国家有关规定”，后者的范围明显更广。根据刑法第九十六条的规定，“国家规定”仅限于全国人大及其常委会制定的法律和决定，国务院制定的行政法规、规定的行政措施、发布的决定和命令。**而“国家有关规定”还包括部门规章，这些规定散见于金融、电信、交通、教育、医疗、统计、邮政等领域的法律、行政法规或部门规章中。**

(三) 对“非法获取”的审查认定

在窃取或者以其他方法非法获取公民个人信息的行为中，需要着重把握“其他方法”的范围问题。**“其他方法”，是指“窃取”以外，与窃取行为具有同等危害性的方法，其中，购买是最常见的非法获取手段。**侵犯公民个人信息犯罪作为电信网络诈骗的上游犯罪，诈骗分子往往先通过网络向他人购买公民个人信息，然后自己直接用于诈骗或转发给其他同伙用于诈骗，诈骗分子购买公民个人信息的行为属于非法获取行为，其同伙接收公民个人信息的行为明显也属于非法获取行为。同时，一些房产中介、物业管理公司、保险公司、担保公司的业务员往往与同行通过QQ、微信群互相交换各自掌握的客户信息，这种交换行为也属于非法获取行为。此外，行为人在履行职责、提供服务过程中，违反国家有关规定，未经他

人同意收集公民个人信息，或者收集与提供的服务无关的公民个人信息的，也属于非法获取公民个人信息的行为。

（四）对“情节严重”和“情节特别严重”的审查认定

1. 关于“情节严重”的具体认定标准，根据《解释》第五条第一款的规定，主要涉及五个方面：

（1）**信息类型和数量。**①行踪轨迹信息、通信内容、征信信息、财产信息，此类信息与公民人身、财产安全直接相关，数量标准为五十条以上，且仅限于上述四类信息，不允许扩大范围。对于财产信息，既包括银行、第三方支付平台、证券期货等金融服务账户的身份认证信息（一组确认用户操作权限的数据，包括账号、口令、密码、数字证书等），也包括存款、房产、车辆等财产状况信息。

②住宿信息、通信记录、健康生理信息、交易信息等可能影响公民人身、财产安全的信息，数量标准为五百条以上，此类信息也与人身、财产安全直接相关，但重要程度要弱于行踪轨迹信息、通信内容、征信信息、财产信息。对“其他可能影响人身、财产安全的公民个人信息”的把握，应当确保所适用的公民个人信息涉及人身、财产安全，且与“住宿信息、通信记录、健康生理信息、交易信息”在重要程度上具有相当性。③除上述两类信息以外的其他公民个人信息，数量标准为五千条以上。

（2）**违法所得数额。**对于违法所得，可直接以犯罪嫌疑人出售公民个人信息的收入予以认定，不必扣减其购买信息的犯罪成本。同时，在审查认定违法所得数额过程中，应当以查获的银行交易记录、第三方支付平台交易记录、聊天记录、犯罪嫌疑人供述、证人证言综合予以认定，对于犯罪嫌疑人无法说明合法来源的用于专门实施侵犯公民个人信息犯罪的银行账户或第三方支付平台账户内资金收入，可综合全案证据认定为违法所得。

（3）**信息用途。**公民个人信息被他人用于违法犯罪活动的，不要求他人的行为必须构成犯罪，只要行为人明知他人非法获取公民个人信息用于违法犯罪活动即可。

（4）**主体身份。**如果行为人系将在履行职责或者提供服务过程中获得的公民个人信息出售或者提供给他人的，涉案信息数量、违法所得数额只要达到一般主体的一半，即可认为“情节严重”。

（5）**主观恶性。**曾因侵犯公民个人信息受过刑事处罚或者二年内受过行政处罚，又非法获取、出售或者提供公民个人信息的，即可认为“情节严重”。

2. 关于“情节特别严重”的认定标准，根据《解释》，主要分为两类：一是信息数量、违法所得数额标准。二是信息用途引发的严重后果，其中造成人身伤亡、经济损失、恶劣社会影响等后果，需要审查认定侵犯公民个人信息的行为与严重后果间存在因果关系。

对于涉案公民个人信息数量的认定，根据《解释》第十一条，非法获取公民个人信息后又出售或者提供的，公民个人信息的条数不重复计算；向不同单位或者个人分别出售、提供同一公民个人信息的，公民个人信息的条数累计计算；对批量出售、提供公民个人信息的条数，根据查获的数量直接认定，但是有证据证明信息不真实或者重复的除外。在实践中，如犯罪嫌疑人多次获取同一条公民个人信息，一般认定为一条，不重复累计；但获取的该公民个人信息内容发生了变化的除外。

对于涉案公民个人信息数量、社会危害性等因素的审查，应当结合刑法第二百五十三条和《解释》的规定进行综合审查。**涉案公民个人信息数量极少，但造成被害人死亡等严重后果的，应审查犯罪嫌疑人行为与该后果之间的因果关系，符合条件的，可以认定为实施《解释》第五条第一款第十项“其他情节严重的情形”的行为，造成被害人死亡等严重后果，从而认定为“情节特别严重”。**如涉案公民个人信息数量较多，但犯罪嫌疑人仅仅获取而未向他人出售或提供，则可以在认定相关犯罪事实的基础上，审查该行为是否符合《解释》第五条第一款第三、四、五、六、九项及第二款第三项的情形，符合条件的，可以分别认定为“情节严重”“情节特别严重”。

此外，**针对为合法经营活动而购买、收受公民个人信息的行为，在适用《解释》第六条的定罪量刑标准时须满足三个条件：一是为了合法经营活动，对此可以综合全案证据认定，但主要应当由犯罪嫌疑人一方提供相关证据；二是限于普通公民个人信息，即不包括可能影响人身、财产安全的敏感信息；三是信息没有再流出扩散，即行为方式限于购买、收受。**如果将购买、收受的公民个人信息非法出售或者提供的，定罪量刑标准应当适用《解释》第五条的规定。

（五）对关联犯罪的审查认定

对于侵犯公民个人信息犯罪与电信网络诈骗犯罪相交织的案件，应严格按照《最高人民法院、最高人民检察院、公安部关于办理电信网络诈骗等刑事案件适用法律若干问题的意见》（法发〔2016〕32号）的规定进行审查认定，即通过认真审查非法获取、出售、提供公民个人信息的犯罪嫌疑人对电信网络诈骗犯罪的参与程度，结合能够证实其认知能力的学历文化、聊天记录、通话频率、获取固定报酬还是参与电信网络诈骗犯罪分成等证据，分析判断其是否属于诈骗共同犯罪、是否应该数罪并罚。

根据《解释》第八条的规定，**设立用于实施出售、提供或者非法获取公民个人信息违法犯罪活动的网站、通讯群组，情节严重的，应当依照刑法第二百八十七条之一的规定，以非法利用信息网络罪定罪；同时构成侵犯公民个人信息罪的，应当认定为侵犯公民个人信息罪。**

对于违反国家有关规定，采用技术手段非法侵入合法存储公民个人信息的单位数据库窃取公民个人信息的行为，也符合刑法第二百八十五条第二款非法获取计算机信息系统数据罪的客观特征，**同时触犯侵犯公民个人信息罪和非法获取计算机信息系统数据罪的，应择一重罪论处。**

此外，针对公安民警在履行职责过程中，违反国家有关规定，查询、提供公民个人信息的情形，应当认定为“违反国家有关规定，将在履行职责或者提供服务过程中以其他方法非法获取或提供公民个人信息”。但同时，应当审查犯罪嫌疑人除该行为之外有无其他行为侵害其他法益，从而对可能存在的其他犯罪予以准确认定。

三、社会危险性及其羁押必要性审查

（一）审查逮捕

- 1. 犯罪动机：**一是出售牟利；二是用于经营活动；三是用于违法犯罪活动。犯罪动机表明犯罪嫌疑人主观恶性，也能证明犯罪嫌疑人是否可能实施新的犯罪。
- 2. 犯罪情节。**犯罪嫌疑人的行为直接反映其人身危险性。具有下列情节的侵犯公民个人信息犯罪，能够证实犯罪嫌疑人主观恶性和人身危险性较大，实施新的

犯罪的可能性也较大,可以认为具有较大的社会危险性:一是犯罪持续时间较长、多次实施侵犯公民个人信息犯罪的;二是被侵犯的公民个人信息数量或违法所得巨大的;三是利用公民个人信息进行违法犯罪活动的;四是犯罪手段行为本身具有违法性或者破坏性,即犯罪手段恶劣的,如骗取、窃取公民个人信息,采取胁迫、植入木马程序侵入他人计算机系统等非法获取信息。**犯罪嫌疑人实施侵犯公民个人信息犯罪,不属于“情节特别严重”,系初犯,全部退赃,并确有悔罪表现的,可以认定社会危险性较小,没有逮捕必要。**

(二) 审查起诉

在审查起诉阶段,要结合侦查阶段取得的事实证据,进一步引导侦查机关加大捕后侦查力度,及时审查新证据。在羁押期限届满前对全案进行综合审查,对于未达到逮捕证明标准的,撤销原逮捕决定。

经羁押必要性审查,发现犯罪嫌疑人具有下列情形之一的,应当向办案机关提出释放或者变更强制措施的建议:

1. 案件证据发生重大变化,没有证据证明有犯罪事实或者犯罪行为系犯罪嫌疑人、被告人所为的。
2. 案件事实或者情节发生变化,犯罪嫌疑人、被告人可能被判处拘役、管制、独立适用附加刑、免于刑事处罚或者判决无罪的。
3. 继续羁押犯罪嫌疑人、被告人,羁押期限将超过依法可能判处的刑期的。
4. 案件事实基本查清,证据已经收集固定,符合取保候审或者监视居住条件的。

经羁押必要性审查,发现犯罪嫌疑人、被告人**具有下列情形之一,且具有悔罪表现,不予羁押不致发生社会危险性的,可以向办案机关提出释放或者变更强制措施的建议:**

1. 预备犯或者中止犯;共同犯罪中的从犯或者胁从犯。
2. 主观恶性较小的初犯。
3. 系未成年人或者年满七十五周岁的人。
4. 与被害方依法自愿达成和解协议,且已经履行或者提供担保的。
5. 患有严重疾病、生活不能自理的。
6. 系怀孕或者正在哺乳自己婴儿的妇女。
7. 系生活不能自理的人的唯一扶养人。
8. 可能判处一年以下有期徒刑或者宣告缓刑的。
9. 其他不需要继续羁押犯罪嫌疑人、被告人的情形。

(三) 最高人民法院 最高人民检察院 公安部《关于办理信息网络犯罪案件适用刑事诉讼程序若干问题的意见》【法发(2022)23号】(2022.08.26 发布 2022.09.01 实施)

为依法惩治信息网络犯罪活动,根据《中华人民共和国刑法》《中华人民共和国刑事诉讼法》以及有关法律、司法解释的规定,结合侦查、起诉、审判实践,现就办理此类案件适用刑事诉讼程序问题提出以下意见。

一、关于信息网络犯罪案件的范围

1.本意见所称信息网络犯罪案件包括:

- (1) 危害计算机信息系统安全犯罪案件;

(2) 拒不履行信息网络安全管理义务、非法利用信息网络、帮助信息网络犯罪活动的犯罪案件；

(3) 主要行为通过信息网络实施的诈骗、赌博、侵犯公民个人信息等其他犯罪案件。

二、关于信息网络犯罪案件的管辖

2. 信息网络犯罪案件由犯罪地公安机关立案侦查。必要时，可以由犯罪嫌疑人居住地公安机关立案侦查。

信息网络犯罪案件的犯罪地包括用于实施犯罪行为的网络服务使用的服务器所在地，网络服务提供者所在地，被侵害的信息网络系统及其管理者所在地，犯罪过程中犯罪嫌疑人、被害人或者其他涉案人员使用的信息网络系统所在地，被害人被侵害时所在地以及被害人财产遭受损失地等。

涉及多个环节的信息网络犯罪案件，犯罪嫌疑人为信息网络犯罪提供帮助的，其犯罪地、居住地或者被帮助对象的犯罪地公安机关可以立案侦查。

3. 有多个犯罪地的信息网络犯罪案件，由最初受理的公安机关或者主要犯罪地公安机关立案侦查。有争议的，按照有利于查清犯罪事实、有利于诉讼的原则，协商解决；经协商无法达成一致的，由共同上级公安机关指定有关公安机关立案侦查。需要提请批准逮捕、移送审查起诉、提起公诉的，由立案侦查的公安机关所在地的人民检察院、人民法院受理。

4. 具有下列情形之一的，公安机关、人民检察院、人民法院可以在其职责范围内并案处理：

(1) 一人犯数罪的；

(2) 共同犯罪的；

(3) 共同犯罪的犯罪嫌疑人、被告人还实施其他犯罪的；

(4) 多个犯罪嫌疑人、被告人实施的犯罪行为存在关联，并案处理有利于查明全部案件事实的。

对为信息网络犯罪提供程序开发、互联网接入、服务器托管、网络存储、通讯传输等技术支持，或者广告推广、支付结算等帮助，涉嫌犯罪的，可以依照第一款的规定并案侦查。

有关公安机关依照前两款规定并案侦查的案件，需要提请批准逮捕、移送审查起诉、提起公诉的，由该公安机关所在地的人民检察院、人民法院受理。

5. 并案侦查的共同犯罪或者关联犯罪案件，犯罪嫌疑人人数众多、案情复杂的，公安机关可以分案移送审查起诉。分案移送审查起诉的，应当对并案侦查的依据、分案移送审查起诉的理由作出说明。

对于前款规定的案件，人民检察院可以分案提起公诉，人民法院可以分案审理。分案处理应当以有利于保障诉讼质量和效率为前提，并不得影响当事人质证权等诉讼权利的行使。

6. 依照前条规定分案处理，公安机关、人民检察院、人民法院在分案前有管辖权的，分案后对相关案件的管辖权不受影响。根据具体情况，分案处理的相关案件可以由不同审级的人民法院分别审理。

7. 对于共同犯罪或者已并案侦查的关联犯罪案件，部分犯罪嫌疑人未到案，但不影响对已到案共同犯罪或者关联犯罪的犯罪嫌疑人、被告人的犯罪事实认定的，可以先行追究已到案犯罪嫌疑人、被告人的刑事责任。之前未到案的犯罪嫌疑人、

被告人归案后，可以由原办案机关所在地公安机关、人民检察院、人民法院管辖其所涉及的案件。

8.对于具有特殊情况，跨省（自治区、直辖市）指定异地公安机关侦查更有利于查清犯罪事实、保证案件公正处理的重大信息网络犯罪案件，以及在境外实施的信息网络犯罪案件，公安部可以商最高人民检察院和最高人民法院指定侦查管辖。

9.人民检察院对于审查起诉的案件，按照刑事诉讼法的管辖规定，认为应当由上级人民检察院或者同级其他人民检察院起诉的，应当将案件移送有管辖权的人民检察院，并通知移送起诉的公安机关。人民检察院认为需要依照刑事诉讼法的规定指定审判管辖的，应当协商同级人民法院办理指定管辖有关事宜。

10.犯罪嫌疑人被多个公安机关立案侦查的，有关公安机关一般应当协商并案处理，并依法移送案件。协商不成的，可以报请共同上级公安机关指定管辖。

人民检察院对于审查起诉的案件，发现犯罪嫌疑人还有犯罪被异地公安机关立案侦查的，应当通知移送审查起诉的公安机关。

人民法院对于提起公诉的案件，发现被告人还有其他犯罪被审查起诉、立案侦查的，可以协商人民检察院、公安机关并案处理，但可能造成审判过分迟延的除外。决定对有关犯罪并案处理，符合《中华人民共和国刑事诉讼法》第二百零四条规定的，人民检察院可以建议人民法院延期审理。

三、关于信息网络犯罪案件的调查核实

11.公安机关对接受的案件或者发现的犯罪线索，在审查中发现案件事实或者线索不明，需要经过调查才能够确认是否达到刑事立案标准的，经公安机关办案部门负责人批准，可以进行调查核实；经过调查核实达到刑事立案标准的，应当及时立案。

12.调查核实过程中，可以采取询问、查询、勘验、检查、鉴定、调取证据材料等不限制被调查对象人身、财产权利的措施，不得对被调查对象采取强制措施，不得查封、扣押、冻结被调查对象的财产，不得采取技术侦查措施。

13.公安机关在调查核实过程中依法收集的电子数据等材料，可以根据有关规定作为证据使用。

调查核实过程中收集的材料作为证据使用的，应当随案移送，并附批准调查核实的相关材料。

调查核实过程中收集的证据材料经查证属实，且收集程序符合有关要求的，可以作为定案依据。

四、关于信息网络犯罪案件的取证

14.公安机关向网络服务提供者调取电子数据的，应当制作调取证据通知书，注明需要调取的电子数据的相关信息。调取证据通知书及相关法律文书可以采用数据电文形式。跨地域调取电子数据的，可以通过公安机关信息化系统传输相关数据电文。

网络服务提供者向公安机关提供电子数据的，可以采用数据电文形式。采用数据电文形式提供电子数据的，应当保证电子数据的完整性，并制作电子证明文件，载明调证法律文书编号、单位电子公章、完整性校验值等保护电子数据完整性方法的说明等信息。

数据电文形式的法律文书和电子证明文件，应当使用电子签名、数字水印等方式保证完整性。

15. 询（讯）问异地证人、被害人以及与案件有关联的犯罪嫌疑人的，可以由办案地公安机关通过远程网络视频等方式进行并制作笔录。

远程询（讯）问的，应当由协作地公安机关事先核实被询（讯）问人的身份。办案地公安机关应当将询（讯）问笔录传输至协作地公安机关。询（讯）问笔录经被询（讯）问人确认并逐页签名、捺指印后，由协作地公安机关协作人员签名或者盖章，并将原件提供给办案地公安机关。询（讯）问人员收到笔录后，应当在首页右上方写明“于某年某月某日收到”，并签名或者盖章。

远程询（讯）问的，应当对询（讯）问过程同步录音录像，并随案移送。

异地证人、被害人以及与案件有关联的犯罪嫌疑人亲笔书写证词、供词的，参照执行本条第二款规定。

16. 人民检察院依法自行侦查、补充侦查，或者人民法院调查核实相关证据的，适用本意见第 14 条、第 15 条的有关规定。

17. 对于依照本意见第 14 条的规定调取的电子数据，人民检察院、人民法院可以通过核验电子签名、数字水印、电子数据完整性校验值及调证法律文书编号是否与证明文件相一致等方式，对电子数据进行审查判断。

对调取的电子数据有疑问的，由公安机关、提供电子数据的网络服务提供者作出说明，或者由原调取机关补充收集相关证据。

五、关于信息网络犯罪案件的其他问题

18. 采取技术侦查措施收集的材料作为证据使用的，应当随案移送，并附采取技术侦查措施的法律文书、证据材料清单和有关说明材料。

移送采取技术侦查措施收集的视听资料、电子数据的，应当由两名以上侦查人员制作复制件，并附制作说明，写明原始证据材料、原始存储介质的存放地点等信息，由制作人签名，并加盖单位印章。

19. 采取技术侦查措施收集的证据材料，应当经过当庭出示、辨认、质证等法庭调查程序查证。

当庭调查技术侦查证据材料可能危及有关人员的人身安全，或者可能产生其他严重后果的，法庭应当采取不暴露有关人员身份和技术侦查措施使用的技术设备、技术方法等保护措施。必要时，审判人员可以在庭外对证据进行核实。

20. 办理信息网络犯罪案件，对于数量特别众多且具有同类性质、特征或者功能的物证、书证、证人证言、被害人陈述、视听资料、电子数据等证据材料，确因客观条件限制无法逐一收集的，应当按照一定比例或者数量选取证据，并对选取情况作出说明和论证。

人民检察院、人民法院应当重点审查取证方法、过程是否科学。经审查认为取证不科学的，应当由原取证机关作出补充说明或者重新取证。

人民检察院、人民法院应当结合其他证据材料，以及犯罪嫌疑人、被告人及其辩护人所提辩解、辩护意见，审查认定取得的证据。经审查，对相关事实不能排除合理怀疑的，应当作出有利于犯罪嫌疑人、被告人的认定。

21. 对于涉案人数特别众多的信息网络犯罪案件，确因客观条件限制无法收集证据逐一证明、逐人核实涉案账户的资金来源，但根据银行账户、非银行支付账户等交易记录和其他证据材料，足以认定有关账户主要用于接收、流转涉案资金的，可以按照该账户接收的资金数额认定犯罪数额，但犯罪嫌疑人、被告人能够作出合理说明的除外。案外人提出异议的，应当依法审查。

22.办理信息网络犯罪案件，应当依法及时查封、扣押、冻结涉案财物，督促涉案人员退赃退赔，及时追赃挽损。

公安机关应当全面收集证明涉案财物性质、权属情况、依法应予追缴、没收或者责令退赔的证据材料，在移送审查起诉时随案移送并作出说明。其中，涉案财物需要返还被害人的，应当尽可能查明被害人损失情况。人民检察院应当对涉案财物的证据材料进行审查，在提起公诉时提出处理意见。人民法院应当依法作出判决，对涉案财物作出处理。

对应当返还被害人的合法财产，权属明确的，应当依法及时返还；权属不明的，应当在人民法院判决、裁定生效后，按比例返还被害人，但已获退赔的部分应予扣除。

23.本意见自 2022 年 9 月 1 日起施行。《最高人民法院、最高人民检察院、公安部关于办理网络犯罪案件适用刑事诉讼程序若干问题的意见》（公通字〔2014〕10 号）同时废止。

最高人民法院 最高人民检察院
公安部

2022 年 8 月 26 日

（四）最高人民法院 最高人民检察院 公安部《关于依法惩治网络暴力违法犯罪的指导意见》【法发〔2023〕14 号】2023.09.20 发布 2023.09.20 实施

4.依法惩治侵犯公民个人信息行为。**组织“人肉搜索”，违法收集并向不特定多数人发布公民个人信息，情节严重，符合刑法第二百五十三条之一规定的，以侵犯公民个人信息罪定罪处罚；**依照刑法和司法解释规定，同时构成其他犯罪的，依照处罚较重的规定定罪处罚。

（五）最高人民法院、最高人民检察院、公安部《关于办理电信网络诈骗等刑事案件适用法律若干问题的意见（二）》【法发〔2021〕22 号】（2021.06.17 发布 2021.06.17 实施）

五、非法获取、出售、提供具有信息发布、即时通讯、支付结算等功能的互联网账号密码、个人生物识别信息，符合刑法第二百五十三条之一规定的，以侵犯公民个人信息罪追究刑事责任。

对批量前述互联网账号密码、个人生物识别信息的条数，根据查获的数量直接认定，但有证据证明信息不真实或者重复的除外。

（六）最高人民法院、最高人民检察院、公安部《办理跨境赌博犯罪案件若干问题的意见》【公通字〔2020〕14 号】（2020.10.16 发布，2020.10.16 实施）

四、关于跨境赌博关联犯罪的认定

.....

（五）为赌博犯罪提供资金、信用卡、资金结算等服务，构成赌博犯罪共犯，同时构成非法经营罪、妨害信用卡管理罪、窃取、收买、非法提供信用卡信息罪、掩饰、隐瞒犯罪所得、犯罪收益罪等罪的，依照处罚较重的规定定罪处罚。

为网络赌博犯罪提供互联网接入、服务器托管、网络存储、通讯传输等技术支持，或者提供广告推广、支付结算等帮助，构成赌博犯罪共犯，同时构成非法利用信息网络罪、帮助信息网络犯罪活动罪等罪的，依照处罚较重的规定定罪处罚。

为实施赌博犯罪，非法获取公民个人信息，或者向实施赌博犯罪者出售、提供公民个人信息，构成赌博犯罪共犯，同时构成侵犯公民个人信息罪的，依照处罚较重的规定定罪处罚。

（七）最高人民法院《人民法院落实〈保护司法人员依法履行法定职责规定〉的实施办法》【法发〔2017〕4号】（2017.02.07 发布，2017.02.07 实施）

第十二条 对于泄露、传播依法不应当公开的法官或其近亲属信息，以及偷窥、偷拍、窃听、散布法官或其近亲属隐私的行为人，人民法院应当商请公安机关依法处理；构成侵犯公民个人信息罪等犯罪的，依法追究刑事责任。

人民法院应当充分发挥诉讼服务中心、12368 诉讼服务平台和诉讼服务网站等平台查询信息、答复咨询、联系法官的作用，避免因信息过度公开影响法官的审判工作和日常生活。通过审判流程信息公开平台对外公开法官姓名、照片、职务、等级、办公电话和工作邮箱之外信息的，应当征得法官本人同意。

（八）最高人民法院 最高人民检察院 公安部《关于办理医保骗保刑事案件若干问题的指导意见》【法发〔2024〕6号】（2024.02.28 发布 2024.02.28 实施）

11.办理医保骗保刑事案件，要同步审查洗钱、侵犯公民个人信息等其他犯罪线索，实现全链条依法惩治。要结合常态化开展扫黑除恶专项斗争，发现、识别医保骗保团伙中可能存在的黑恶势力，深挖医保骗保犯罪背后的腐败和“保护伞”，并坚决依法严惩。

规范性文件

(一)公安部、北京市网络行业协会《互联网个人信息安全保护指南》(2019.04.10 发布 2019.04.10 实施)

1 范围

本文件制定了个人信息安全保护的管理机制、安全技术措施和业务流程。适用于个人信息持有者在个人信息生命周期处理过程中开展安全保护工作参考使用。本文件适用于通过互联网提供服务的企业，也适用于使用专网或非联网环境控制和处理个人信息的组织或个人。

.....

3 术语和定义

3.1 个人信息

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。

注：个人信息还包括通信通讯联系方式、通信记录和内容、账号密码、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息等。