Advances in Social Sciences 社会科学前沿, 2025, 14(1), 433-440
Published Online January 2025 in Hans. https://www.hanspub.org/journal/ass
https://doi.org/10.12677/ass.2025.141055

Hans汉斯

论侵犯公民个人信息罪“情节严重”的认定

王宇洁

苏州大学王健法学院，江苏 苏州

收稿日期：2024年12月10日；录用日期：2025年1月16日；发布日期：2025年1月26日

摘　要

侵犯公民个人信息罪以“情节严重”为定罪要件要素，对于情节严重的认定引发了刑法学界的争论与分歧。面对个人信息三级分类法的制度缺陷、以“组”代“条”的计算单位争议、批量信息举证与真伪核查的处理难题，本文通过剖析相关法律条文和司法解释，搜寻侵犯公民个人信息罪的现实案例，对调整信息三级分类规范，明确信息数量计算“识别性”标准及统一批量信息推定规则和信息处理模式等破解思路进行了集中阐述，以期进一步改善“情节严重”认定混乱的司法现状。

关键词

侵犯公民个人信息罪，情节严重，司法认定

On the Determination of “Severe Circumstances” in the Crime of Infringing Citizens’ Personal Information

Yujie Wang

Kenneth Wang School of Law, Soochow University, Suzhou Jiangsu

Received: Dec. 10th, 2024; accepted: Jan. 16th, 2025; published: Jan. 26th, 2025

Abstract

The crime of infringing personal information of citizens takes “severe circumstances” as an element of conviction, and the determination of severe circumstances has triggered debates and disagreements in the criminal law academic circle. In the face of the systematic defects of the three-level classification of personal information, the controversy over the calculation unit of “group” instead of “article”, and the difficulties in handling the proof and authenticity verification of bulk information, this paper, through analyzing relevant legal provisions and judicial interpretations, searches

文章引用: 王宇洁. 论侵犯公民个人信息罪“情节严重”的认定[J]. 社会科学前沿, 2025, 14(1): 433-440.
DOI: 10.12677/ass.2025.141055

for real cases of crimes against citizens' personal information, and focuses on such cracking ideas as adjusting the norms of three-level classification of information, clarifying the standard of "identifiability" for calculating the quantity of information, and unifying the rules of presumption of bulk information and the mode of information processing, with a view to improving the confusing judicial the current situation.

Keywords

Infringement of Citizens' Personal Information, Severe Circumstances, Judicial Determination

1. 引言

随着计算机技术和通讯技术的发展，信息在当代社会的重要性日益彰显。个人信息更是凭借其可观的商业经济价值与社会管理价值，获得“新型石油”[1]“数据黄金”[2]的称号。在各种不法利益的驱动下，侵犯公民个人信息的犯罪活动层出叠现，相关黑灰产业链条威胁公民人身、财产安全，紊乱了正常的国家信用体系，危害了社会的管理秩序。为构建完善的个人信息安全法律体系，社会各界期待呼吁良久的前置法《个人信息保护法》终于颁布，在当前刑法、民法和行政法多领域、多部门交叉保障公民个人信息权的中国特色立法背景下，刑法如何遵循法秩序统一原则，如何协调对侵犯公民个人信息罪的规制，使这一典型情节犯的认定标准清晰化，破解“情节严重”这一司法认定的难题，值得我们关注和思考。

2. 侵犯公民个人信息罪“情节严重”的含义与认定依据

要想破解侵犯公民个人信息罪中情节严重的司法认定难题，首先就得理解“情节严重”这一抽象术语在该具体罪名语境中的含义，再探寻相关规范性法律文件中情节严重的认定依据，了解立法现状，抓住症结所在，才能做到有的放矢、直达病灶。

2.1. 侵犯公民个人信息罪“情节严重”的含义

根据《中华人民共和国刑法》(以下简称《刑法》)第 253 条之一，成立侵犯公民个人信息罪是指行为人违反国家有关规定，向他人出售、提供或者以窃取等方法非法获取公民个人信息，构成情节严重的。从犯罪构成来看，首先，该罪分布在《刑法》分则第四章“侵犯公民人身权利、民主权利罪”中，犯罪客体为个人法益，具体而言是个人信息权，包括信息自决权和信息中蕴含的人身、财产、隐私安全。其次，16 周岁以上的自然人和单位都为侵犯公民个人信息罪的行为主体，且对单位实行“双罚制”。再次，主观方面为故意，过失不为罪。最后，危害行为作为侵犯公民个人信息罪客观方面的重要构成要素，可分为“提供型”和“非法获取型”，“提供型”包括有偿提供(出售)和无偿提供两种；“非法获取型”又可分为窃取和其他非法获取方法(如购买、交换、侵入他人计算机信息系统实施非法获取行为的)，且要符合“情节严重”的要求。

那么，如何理解这里的“情节严重”呢？从刑法理论上来说，“情节严重”在具体罪名中，包含定罪情节和量刑情节两类。其中，“情节严重”作为定罪情节，是犯罪客观方面的构成要件要素，通过客观方面体现法益的侵害程度，起到区分罪与非罪的作用；而“情节严重”作为量刑情节，不是犯罪构成的组

成部分，而是法定刑的升格条件，起到区分重罪和轻罪的作用。显然对于侵犯个人信息罪而言，“情节严重”属于定罪情节，即唯有从事了《刑法》第253条之一规定的侵犯行为，且具有相当的社会危害性，达到“情节严重”的程度，才启用刑罚手段予以谴责。

2.2. 侵犯公民个人信息罪“情节严重”的认定依据

在我国刑法分则各种犯罪构成的具体规定中，“情节严重”、“情节恶劣”是很多罪名的成立要件，形成了独特的定罪标准。刑法学界一般将这些以“情节严重”、“情节恶劣”作为入罪必备条件的犯罪，称之为“情节犯”。因此，侵犯公民个人信息罪属于典型的情节犯。这种我国独创的立法模式灵活区分了治安管理处罚和刑罚手段，充分体现了刑法作为维护法治最后一道防线的谦抑性。

但与此同时，本罪中“情节严重”这一罪状特征的概括性往往会导致司法认定不一致，裁判结果相冲突。为此，2017年《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》(以下简称《解释》)融合信息数量、信息用途、营利金额、违法所得等多项指标，以期指导、统一法治工作队伍对“情节严重”的认定。其中，侵犯公民个人信息的具体数量在一定程度上最为直观明显地反映了侵犯范围和社会危害程度，是衡量“情节严重”、定罪量刑的有力准绳。在实务工作中，以信息数量作为主要认定标准的判决书屡见不鲜，占到了差不多一半的认定比例。

《解释》第五条第一款第(三)至(五)项依照信息与人身、财产安全间的关联性和重要性，将公民个人信息分为三类，分别按不同的数量梯度制定入罪门槛——“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”为第一层级，这四种信息识别性强，指向性高，一旦泄露就会直接威胁到特定自然人的人身、财产法益，极易引发诈骗、敲诈勒索、绑架等社会危害性较大的下游犯罪，因此刑法保护必要性和紧迫性最高，50条以上即构成“情节严重”；“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”为第二层级，侵犯列举的这四种信息及其他与之重要程度相当、较易锁定受害人身份的个人信息，500条以上构成“情节严重”；“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”为第三层级，属于兜底条款，该层级对信息重要程度要求最低，一般需要不同信息间的组合才能识别具体身份，对人身、财产权益损害较为轻微，5000条以上才构成“情节严重”。

观察《解释》第五条第一款第(三)至(五)项，参考刑法理论界通说，可将50条、500条和5000条依次递增组成的三个梯度，分别命名为高度敏感信息、一般敏感信息和非敏感信息，实现对情节严重的认定。

3. 侵犯公民个人信息罪“情节严重”的司法认定难题

虽然分类定罪、分级保护的司法解释技术丰富了司法操作中的细则，看似清晰，使司法部门对侵犯公民个人信息的犯罪行为定罪量刑有据可依，但因其中涵摄了更多意义模糊的下位概念，也给法官留下过大的自由裁量缺口，在实际审判中因理解各异，对“情节严重”认定分歧的痼疾依旧存在，同案异判，类案失衡的情形仍然时有发生。同时，随着2021年11月1日专门法《个人信息保护法》呱呱坠地、正式实施，其对于整个个人信息法律保护体系的影响与冲击不容小觑，涉及刑法与行政法衔接、新旧法协调适用的热点问题也纷纷呈现，亟待解决。据笔者观察，在对公民个人信息保护过程中比较明显的问题存在于信息分类、信息计算、信息真伪核查等方面。

3.1. 信息分类制度缺陷

《个人信息保护法》延续了《解释》对个人信息分类保护的基本思路，但与《解释》三级分类法相异，《个人信息保护法》对个人信息采用了“二分法”，着重考虑了不同信息的客观权益侵害风险和法律

规制敏感程度，将个人信息分成敏感信息和一般信息。根据该法第二十八条第一款的规定，前者是指“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。”可见敏感信息涵盖了人身、财产权益最易受侵害的信息种类，同时也充分顾及到14周岁以下未成年人信息控制能力有限、隐私暴露风险大的特征，给予此类信息严格的保护。而除此之外，保护程度相对较弱的则为一般信息。比较“二分法”和原有的三级分类法，《解释》似有不尽合理之处。

其一，三级分类法中对高度敏感信息的保护存在滞后性，处罚范围有过窄之嫌。在第一层级中，《解释》采封闭式列举，将高度敏感信息严格限定于行踪轨迹信息、通信内容、征信信息、财产信息四种。然而，实质上认定高度敏感信息的核心要素为是否与人身、财产安全最直接关联，那么该四种信息类型有无覆盖周延？特别是现代社会指纹解锁、面部识别运用广泛，利用人体先天具有、不可复制的生理特性来鉴别身份的生物识别技术日益发达，由于生物识别信息具有定位唯一性，又密切关系到公民个人的核心隐私和重要资产安全，已被《个人信息保护法》纳入敏感信息，作为重点保护对象，刑法对此却未直接回应，态度隐晦。因此，严守罪刑相当原则，推进刑法对生物识别信息的精准归类势在必行。

其二，三级分类法难以将融合度较高的信息进行精准分类。大数据的时代背景意味着海量信息的存在，更意味着各种不同类型数据的多元融合，往往一条信息由多条信息的内容交织整合而成，承载着丰富的人身、财产价值，复杂程度超出了三级分类法的界定标准。如新冠肺炎疫情期间人们使用的“健康码”[3]。健康码是反映个人身体健康状况的电子凭证，疫苗接种情况、核酸检测数据都被囊括其中，可被归入第二层级一般敏感信息的“健康生理信息”；随着“互联网 + 医疗健康”行业不断成熟，为方便人员一码通行与跨省流动，国家政务平台已整合“通信大数据行程卡”相关信息，用户是否去过中高风险地区等行程信息可直接显示在健康码中，能清晰反映个人的活动情况，因此健康码又可被归入第一层级的“行踪轨迹信息”。那么严重侵犯健康码信息的违法犯罪活动究竟该由《解释》第五条第一款第三项还是第四项惩治呢？像这种信息内容交叉、重合的问题，司法认定中常常莫衷一是。

其三，三级分类法存在对信息分类的“一刀切”而与危害性失衡的情形。《解释》在将个人的行踪轨迹信息等四类信息定义为高度敏感信息，但这类信息的内容只有达到一旦泄露、对公民个人利益的潜在危害性达到一定程度才有予以刑罚追究的意义。如，某人某天偶发至某商场的一次已经结束的购物活动行踪轨迹，从中既不能获取某人的实时位置，亦不足以发现该人的日常行为规律或依此形成对该人个性化的识别。但如果某人连续数月甚至多年购物的习惯性轨迹，则可以对某人产生身份的识别并对将来行踪形成预判。在此类事件中，一次性行踪信息的危险性远不如长期的行踪的归纳的信息，但三级分类法并未对此再作区别。类推及其他，一片碎片化的信息可能属于三分法所指的敏感信息的类型，但只有一定数量的碎片才能组合构成足以产生与侵犯公民个人信息犯罪归类所需的具有潜在危害的信息。

3.2. 信息计算单位争议

“条”作为计算信息数量的基本单位，是判断是否构成情节犯的关键度量衡，而在现实生活中，有不止一例判决以“组”替代“条”来衡量信息数量。如在(2021)苏0206刑初668号判决中，审判员详述了被告人张某宇通过微信和QQ向他人出售名为“100.TXT”的邮箱账号及对应密码等公民个人信息的文件999,987组[1]；在(2021)鲁09刑终14号判决中，上诉人李某使用嗅探设备，非法获取他人信息包括姓名、电话号码、身份证号码三项在内共计158组[2]。可见，“组”往往是指多种不同类型的个人信息、最终作为一个整体使用的组合，可以是邮箱账号加密码为一组，也可以是姓名加电话号码加身份证号码

[1](2021)苏0206刑初668号，江苏省无锡市惠山区人民法院：“张航宇侵犯公民个人信息罪刑事一审刑事判决书”。

[2](2021)鲁09刑终14号，山东省泰安市中级人民法院：“李政信用卡诈骗二审刑事判决书”。

为一组，只要能相互结合共同指向某一特定公民，就计为一组，不重复累计。

面对上述司法解释与法律实务、应然规定与实然状态的差异，有学者表示组和条看似是相近的数量单位，但是实际上仍然存在差别，是否能将其等同适用仍然缺乏明确的规定；有学者建议在计算个人信息条数的过程中，采取“组”的概念，来替代“条”的认定，能够有效避免将重复信息叠加计算的情形。刑法学界对计算单位的认定观点不一，进一步明确公民个人信息数量的计算标准，已成为当务之急。

3.3. 信息真伪核查难题

批量信息的真伪核实问题对众多司法工作人员来说一向棘手，实务工作中也没有统一的认定标准。《解释》第十一条第三款规定：“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。”该款是否为举证责任倒置的体现？是否应由被告人承担对个人信息真实性的证明责任？

现实中有检察机关对该困惑做出了肯定回答，未对批量信息做任何处理，按照获取的信息数量直接认定。如将被告人手机、电脑等移动终端里储存的所有“公民个人信息”通通计算在内，不分用途，不加区分，按图索骥匹配相应层级的数量梯度。虽然该做法极大地提升了结案速度，但其产生的误差无法估量；也有检察机关按程序查证、核实信息，举证确实充分，如在尹某同侵犯公民个人信息罪一案中，无锡市惠山区人民法院对被告人尹某同购买的链接内含公民身份证照片、公民手持身份证照片等 39,017 条公民个人信息合并去重，真实有效的信息数量为 4915 条[3]；在王某杰侵犯公民个人信息罪一案中，上海市第二中级人民法院从二共犯扣押的手机、电脑中共检出原始数据信息 81,159 条，而汇总、去重后检出真实有效的数据为 51,551 条[4]。可见如果不经过查证和处理，原始信息和真实信息数额相距甚远，严重影响了定罪量刑的幅度。解决同案不同判这一广为诟病的实务难题迫在眉睫。

上述冲突，无论是个人信息分类的二分法与三分法之间的冲突，还是三分法中信息性质与数量、数量的计算单位“条”与“组”、真伪信息之间的冲突，都给侵犯公民个人信息情节严重的司法认定带来困惑与困难。

4. 侵犯公民个人信息罪“情节严重”认定难题的破解思路

“情节严重”是侵犯公民个人信息罪在定罪量刑环节都要直接面对的问题，而目前刑法分则的规定和司法解释的补充都没有完全解决所存在的信息识别与计算问题。针对《解释》中个人信息三级分类法的制度缺陷、以“组”代“条”的计算单位争议、批量信息举证与真伪核查的处理难题，笔者提出以下建议和完善措施。

4.1. 调整信息三级分类规范

其一，科学界定信息内涵。仅凭《解释》第一层级中原有的四类信息无法穷尽高度敏感信息。笔者建议借鉴对一般敏感信息的规定，采用概括加列举、形式标准和实质标准相结合的规范方式——在四类信息后加上“等”字，作为列举未尽的“等外等”，以示前瞻性；同时补充对高度敏感信息本质特征“直接影响人身、财产安全”的表述，完善《解释》第五条第一款第三项为“非法获取、出售或者提供行踪轨迹信息、通信内容、征信信息、财产信息等直接影响人身、财产安全的公民个人信息五十条以上的”。这样既注重立法语言结构的统一美感，又有效防止了封闭区间对信息种类的遗漏评价，使得分类标准体系性、严谨性、灵活性三者有机统一。

[3](2021)苏 0206 刑初 741 号，江苏省无锡市惠山区人民法院：“尹鸿同侵犯公民个人信息罪刑事一审刑事判决书”。

[4](2021)沪 02 刑终 245 号，上海市第二中级人民法院：“暨原审附带民事公益诉讼被告人王耀杰侵犯公民个人信息二审刑事裁定书”。

若以该标准判断生物识别信息的归属，分类疑难则能迎刃而解。鉴于生物识别信息定位唯一性、难更改性和可作密码性的显著特征，诸如指纹支付密码等生物识别信息一旦被盗取、出售或滥用，对人身、财产权益所造成的损害往往持久难消、不可逆转，因此生物识别信息符合高度敏感信息的本质特征，刑法保护必要性和紧迫性与行踪轨迹信息等四类信息相当，属于“等外等”的内容，应归入三级分类法中的第一层级，最为严格地限制侵犯数量。

其二，从严认定交叉重合的信息。关于内容交叉重合的信息，想要准确认定数据类型，笔者认为可以参照周光权教授关于手机位置信息归类的观点。他指出，如果行为人通过一定程序能够获取未经个人授权的手机号码位置信息的，该信息既属于行踪轨迹信息，也属于通讯记录，应当将其作为高度敏感信息予以保护[4]。从学理上来说，这样能有效避免主观定罪的随意性，侧重保护法益，防止轻纵犯罪人。回到上文所举的健康码，客观上健康码兼具“生理健康信息”和“行踪轨迹信息”的属性，可界定为高度敏感信息或一般敏感信息，那么就高不就低，倾向于认定其是第一层级的高度敏感信息是比较合理的。

其三，合并计算碎片化信息。一个信息片段或碎片化信息通常不具有经济价值，或许难以被归入为敏感信息范畴，但多个碎片即能拼凑出可以被不法利用的公民信息。如通过持续跟踪某人的购物信息，可以得出该人的消费习惯、品牌偏好，甚至是收入水平、行动规律等高度敏感信息。因此，在统计符合犯罪信息的类型与数量时，我们既不应该忽视无足轻重的“碎片”，随意抛弃，也不能将无数的“碎片”逐一计算，重复归罪，而应将反映同一公民特征、信息内容未发生变化的“碎片”合并计算。而对于无害化的“碎片”，或暂时不能确定危险性的信息片段，应按疑罪从无的精神，在认定情节严重的信息计量中予以剔除。

4.2. 明确信息数量计算“识别性”标准

欲解决“条”“组”之争，首先我们就得明确计算信息数量的标准。对此《解释》和《个人信息保护法》都秉持了较为一致的“识别性”标准，从两者对公民个人信息的概念表述中即可见一斑。依照《解释》第一条，“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。相应的，《个人信息保护法》第四条第一款指出，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。比较可得二者虽在表述上不尽相同，但本质上对个人信息的认定标准高度重合，都强调信息识别特定自然人的关联程度，依附于与具体个人的紧密性。

遵照“识别性”标准，公民个人信息可分成已识别信息与可识别信息两类。“已识别”即能明确指向某一公民个人，“可识别”则需信息间的相互组合来锁定特定对象。结合《解释》的三级分类制度，一般而言，前两类层级的信息指向性高，直接按“条”评价并无不妥；难点主要出在非敏感信息数量的计算，草率粗暴的简单叠加不可取，不同信息组合成一体定位到唯一的个人，上述司法实践中“组”的计算单位应运而生。

一一考察上文众学者的意见，笔者认为“组”与“条”作为信息数量的计算单位，仅存在文义描述上的不同，不具有实质上的差别。首先，无论是“条”还是“组”，既然均指向同一个体，只要符合“识别性”标准的要求，识别到唯一的自然人，从根本上讲还是只侵害了特定对象的信息自决权，对法益的损害并不以信息种类的不同而叠加计算；其次，“条”“组”都是经过价值评价的信息数量计算单位，应当将其与事实层面计量文书单位的量词区别开，不可以生活视角等同对待。而设置“条”主“组”辅双重单位的观点提出在“组”表示一人一组多条信息时，“组”即为信息数量计算规则中的“条”，而“条”是事实判断中的原始信息单位，分别从事实层面与法律评价层面定义“条”，背离了体系逻辑的一致性，

将原本单一清晰的“识别性”标准复杂化，较为繁琐；最后，在没有法律依据的情况下凭空创造新的基本单位“组”，违背了罪刑法定原则。

综上，坚持传统单位“条”的适用，公检法机关提高对“识别性”标准的重视程度才是解决之道。

4.3. 统一批量信息推定规则与处理模式

首先，《解释》第 11 条第 3 款绝对不是举证责任倒置，而采取了刑事推定。推定，即由基础事实来认定推定事实成立。完成推定后，如没有证据证明信息不真实或重复，推定事实则得以认定。如有不符合推定事实的证据，检方继续承担证明被告人有罪的证明责任，若不能拿出有力的证据进行反驳，将承担被证明信息不真实或重复的不利影响[5]。因此批量信息真实性的证明责任仍应由公诉机关负担，而非被告人。如果公诉机关未收集到确凿充分的证据，举证不能的不利后果就不应由被告人承受，法院就不足以定罪。相反，这作为辩护权的一种延伸，被告人认为信息虚假或重复时，可以随时反驳加以举证。

其次，本规定的目的主要是在云存储技术飞速发展、涉案信息常以百万计的大数据时代，降低公诉方查证全部信息的现实难度，减少办案物质和精神耗费，以最少的司法投入获得最大的诉讼效益。但诉讼经济原则的遵循不应以丧失司法公正性为代价，完全不查重、不去伪存真就直接认定批量个人信息数量的做法理应摈弃。

最后，重视批量信息数量的推定规则、科学合理地计算批量信息的数目，对于缓解核实海量信息的巨大工作量与保障被告人合法权益之间的矛盾，显得极为关键。通过搜索大量关于侵犯公民个人信息罪的相关判决，笔者发现实践中最常用也最有说服力的是分组抽样检测，灵活验证信息的重复率和准确度。以庄某某侵犯公民个人信息罪一案 [5] 为例，浙江省永康市人民法院在一审刑事判决书中详细记录了对批量信息数量进行推定、真伪核实的过程——永康市公安局对被告人庄某某云盘内以千万计的个人信息随机抽取数据文件 116 份，对文件内数据进行筛选，去除重复数据，共提取数据 13 万余条，并以拨打提取到的数据电话向当事人求证的方式核查数据的真实性，共核查数据 1217 条，数据均为真实有效。其中运用了随机抽样——筛选去重——核查信息真实处理模式，笔者深以为然，但如果先对批量信息的来源进行分类，再分组抽取等额样本核实真实性，或许更为完善。

综上，明晰批量信息数量推定规则，全面推广分组抽样的去重、查实处理模式，是批量信息认定难关的关键突破口。

5. 结语

以上论述主要从信息的分级分类及信息条数的统计角度展开，以确认是否成立入罪构成的“情节严重”。不论是刑法及其司法解释的分类标准疏漏，还是公民个人信息数量计算标准模糊，抑或批量信息处理标准理解各异，都已成为“情节严重”司法认定发展道路上的绊脚石，极易导致现实裁判尺度不统一，那么刑法对于公民个人信息的保护就不可能完备周密。《个人信息保护法》的施行，正式填补了我国多年来缺失的前置法漏洞，对刑法来说既是汲取吸收的机遇，也是衔接协调的挑战。据此完善固有的三级分类标准，坚守信息数量“识别性”标准，统一批量信息推定规则和处理模式，才能更加准确地惩治犯罪，维护正义。当然，为了更完整、更客观地评价犯罪行为是否“情节严重”，信息的使用方法、获利情况、主观恶性及对被害人的危害结果等标准亦不能忽略。广泛全面地考察纷繁复杂的个案情节，定性与定量相结合、更加科学地判别“情节严重”，是刑法的应尽之职。这样受益的不仅是刑法部门法内部体系，更促进了整棵个人信息保护法律树的茁壮成长、枝繁叶茂，有利于全方位、多层次、综合性地稳固信息安全的“防火墙”。

[5](2020)浙 0784 刑初 794 号，浙江省永康市人民法院：“庄良焦侵犯公民个人信息罪一审刑事判决书”。

参考文献

[1] 储陈城. 大数据时代个人信息保护与利用的刑法立场转换——基于比较法视野的考察[J]. 中国刑事法杂志, 2019, 5(5): 48-62.

[2] 维克托·迈尔-舍恩伯格, 肯尼斯·库克耶. 大数据时代[M]. 杭州: 浙江人民出版社, 2013: 45.

[3] 刘宪权, 何阳阳. 《个人信息保护法》视角下侵犯公民个人信息罪要件的调整[J]. 华南师范大学学报(社会科学版), 2022(1): 144-154.

[4] 周光权. 侵犯公民个人信息罪的行为对象[J]. 清华法学, 2021, 15(3): 25-40.

[5] 陈瑞华. 论刑事法中的推定[J]. 法学, 2015(5): 105-116.