“人肉开盒”行为的违法判断及民刑共治

赵　龙,王子奇
(烟台大学 法学院,山东 烟台 264005)

摘　要:“人肉开盒”行为是指通过网络收集个人信息,形成可识别的个人画像并公布于网络的行为,包含“人肉”与“开盒”两个环节。目前,“人肉”环节的治理困境主要体现为归责路径模糊,“开盒”环节的治理困境则集中在损害预防失效方面。在民事层面,对平台和“开盒者”行为违法性的分析,主要围绕《个人信息保护法》的规范要求展开;在刑事层面,“人肉开盒”行为及其附随行为可能构成侵犯公民个人信息罪、非法获取计算机信息系统数据罪、非法利用信息网络罪等。“人肉开盒”行为侵害了被害人个人信息权,进而侵害被害人人身财产安全和精神安宁。为实现对法益的周延保护,在民法上应确立个人信息删除权和网络遗忘权制度;在刑法层面,可通过司法解释完善侵犯公民个人信息罪严重情节的罪状描述,追究行为人的刑事责任。

关键词:“人肉开盒”;侵犯公民个人信息罪;法益;民刑共治

中图分类号:D924　　**文献标识码**:A　　**文章编号**:1008-7699(2025)02-0025-09

“人肉开盒”即通过互联网对个人信息进行收集并传播的行为,它不同于早期论坛型平台的“人肉搜索”行为。[1]从性质上看,“人肉开盒”行为是一种社会危害性更高的个人信息泄露行为。“网络与数字技术的发展,摧毁了先前私域与公域之间的物理性边界。”[2]公域中的互联网互动以技术为中介穿透了个人的私域生活,将私生活暴露在互联网的网络凝视与价值评判之下。基于互联网生态与技术的发展,“人肉开盒”行为逐步由以论坛为中心的松散主体针对特定个体的信息收集,演变为组织严密的非法团体通过网络非法批量获取个人信息数据并加以滥用的行为。“人肉开盒”行为的社会危害性逐步增强,为后续电话骚扰、网络暴力乃至网络诈骗等违法犯罪行为提供了温床,具有严重社会危害性。

一、内涵诠释:“人肉开盒”行为的类型化界分

从语义学角度来看,“人肉”即“人肉搜索”的简称,指通过公开方式向网民征集问题答案的行为。[3]后演变为征集个人信息的行为,最终固化为“向网络中的不特定网民征集目标对象个人信息并公布”的行为。随着“人肉”行为信息来源逐渐从网民提供的线索转向数据库,获得个人信息的行为本质与基于网民提供线索的信息汇聚模式逐渐分离,“开盒”成为一种技术化、系统化的新型网络暴力形态。从“人肉”到“开盒”的转变,是对人肉搜索概念的解构与发展。通过对“个人信息聚合与公开”核心要素的抽离与重构,“开盒”被定义为通过网络收集个人信息、形成可识别的个人画像并公布于网络的行为。

(一)以开盒主体为标准的类型划分

根据参与主体特定与否,可将“人肉开盒”行为划分为封闭模式与开放模式。

封闭模式指“人肉开盒”行为的主体相对固定。该模式具有强烈的功利性与目的性,意图通过公布被害人个人信息实现特定利益诉求,其基于利己性意图的行为难以引起网民共鸣,需要依赖严格的中心化组织维系自身存在。该模式下,团体的形成动机源于成员的共同利益或情绪,其价值观与社会通常观念

收稿日期:2024-10-15
基金项目:国家社会科学基金青年项目(24CFX094);2024 年山东省社会科学规划研究一般项目(24CFXJ13)
作者简介:赵　龙(1983—),男,山东曹县人,烟台大学法学院副教授,法学博士.

可能存在冲突。由于组织构成以人际关系为核心,具有强人合性且结构紧密,即使热点事件消退,“人肉开盒”团体仍会持续存在,并反复针对不特定主体实施开盒行为,性质恶劣。

开放模式指“人肉开盒”行为的主体为网络中成员流动性较强的组织,具有大众化、去中心化特征,其既不具有完备组织,也不由特定个人或团体领导。该模式下,个体间不存在上下级关系,也难以产生意见领袖,主体间纽带源自参与者基于情绪、身份等关系产生的归属感,是典型的去中心化网络社群行为。开放模式通过个体情绪凝结各方力量,其产生高度依赖于具体热点事件[4],受害者通常仅限于事件当事人。当事件平息后,该组织会自发解散,相较于封闭模式,社会危害性较小。

(二)以信息收集手段为标准的类型划分

随着技术发展,“人肉开盒”行为形成了传统与现代的两种信息收集模式。传统信息收集模式指开盒者通过人肉搜索、网络爬虫或搜索引擎进行简单检索,汇聚被害人在网络中的零散个人信息,聚合后形成受害者人格画像并予以公布的行为,具有零散性与公开性特征。传统模式中,开盒者独立实施检索、黑客入侵等信息收集行为,因缺少数据库支持而导致实施难度高且效率低下,常出现信息缺失或错误的情况,危害性相对较小。该模式多存在于灰色产业链形成前的网络环境以及网络使用水平较低的“开盒者”群体中。

与传统模式不同,现代信息收集模式基于社工库展开。开盒者仅需以被害人的部分信息在社工库中检索,即可获得被害人的全部数据,此种模式为“人肉开盒”行为提供了前所未有的便利性,具备更强的社会危害性。社工库组织通过收买、网络信息爬取[5]、黑客入侵等非法手段获取数据,经管理者汇总后形成包含海量个人信息的非法数据库,为网络黑产、灰产活动提供服务[6]。

以主体划分的“开盒”模式与以手段划分的信息收集模式呈现交叉态势。开放主体采取传统模式与封闭主体采取现代模式,构成“人肉开盒”行为的主要类型。前者基于网络时代交流的互联性、话题集中性与活动去中心化,可称为“人肉”模式;后者则基于网络技术复杂性与隐匿性,为潜藏于常规社交网络外的黑产、灰产活动提供服务[6],可称为“开盒”模式。“人肉”模式与“开盒”模式均属“人肉开盒”行为的下位概念,其本质是通过互联网非法获取并公布个人信息。

二、治理困境:“人肉开盒”行为的模式化省思

在宏观层面,“人肉开盒”行为治理面临成文法规范缺失的困境[7],既无法有效实现事先预防,也难以落实事后追责。“人肉”模式与“开盒”模式的现实特点差异,导致治理困境各有侧重,同时也为后续规范解释与调整提供了方向。

(一)“人肉”模式的归责路径缺失困境

现行规范未能有效规制“人肉”行为的原因有二:一是,“人肉”行为在早期互联网中处于灰色地带,一般网民难以感知,致使该问题长期处于法治盲区;二是,无论是基于实在规范还是教义学理论,都难以适应“人肉”行为的归责需求。“人肉”模式以高度流动的抽象组织作为社会学意义上的行为“主体”,导致法律在以具体自然人或组织为归责主体时面临困境。从法律适用角度看,人肉活动中单个参与者的侵权行为危害性较低,然而无数行为叠加后,将产生需要法律介入的社会危害。此类行为的归责问题构成“人肉”模式的本质困境。相较之下,对开盒行为,法律可通过打击社工库成员、团体组织者及积极参与者来实现治理。但“人肉”模式全过程缺乏可归责的具体主体。

(二)“开盒”模式的损害预防失效困境

与“人肉”模式不同,“开盒”模式以成员相对固定的团体或个人为行为主体,通过共同利益或目标形成高度中心化组织,能高效实施侵权行为。该模式受害人特征与“人肉”模式存在差异:“人肉”模式受害人基于互联网热点事件产生,“开盒”模式受害者则基于开盒者目的产生,该目的具有高度随意性,导致潜在受害者范围显著大于“人肉”模式。效率层面,高度中心化结构使开盒组织能以极高效率转换侵害目

标,甚至同时侵害多个目标。广泛性与高效性共同导致“人肉开盒”行为的受害人具有随机性特征。相较于网络热点事件的潜在受害人,“开盒”模式受害人因特征不明而难以获得同等规范保护。规范的预防效能随范围扩张与主体特征消弭而降低,对难以预测、控制的开盒行为,规范的事先预防功能难以满足治理的最低要求。

三、民刑分野:“人肉开盒”行为的违法性认定

无论何种模式,“人肉开盒”行为均违背公众普遍道德认知与法律规定,基于我国现行个人信息保护规范体系,对“人肉开盒”行为主要依据《中华人民共和国民法典》(以下简称《民法典》)《中华人民共和国刑法》及《中华人民共和国个人信息保护法》(以下简称《个人信息保护法》)进行规制。

(一)“人肉开盒”行为的民事违法性认定

根据《民法典》及《个人信息保护法》规定,“个人信息处理者”系侵权活动的核心主体。因此,“人肉开盒”行为的民事违法性认定应围绕该主体展开。依据《个人信息保护法》第七十三条第一款①,平台与开盒者均属个人信息处理者。下文将以平台与开盒者为分析对象,探讨“人肉开盒”行为中的民事违法性。

1.“人肉开盒”行为中平台民事违法性认定

平台汇集众多个人信息,是个人信息的主要来源。源自平台的个人信息主要由其雇佣的数据库管理者及使用者泄露,雇员未经信息主体同意处理个人信息具有违法性,但平台的违法性需另行论证。我国个人信息侵权责任属过错责任,平台需具备过错,方构成违法。依据《个人信息保护法》第五十一条,企业应采取权限管理、人员教育培训及加密、去标识化等措施防止信息泄露。平台未履行前述义务的,应认定存在过错且具有违法性。除雇员提供数据外,开盒者还会主动攻击平台数据库非法获取个人信息。平台未履行数据加密或去标识化义务致信息泄露用于开盒的,其不作为行为具违法性。

平台既是“人肉开盒”行为的信息来源,亦系公布被害人个人信息的最终“侵权地”。开盒者在平台公布被害人个人信息,引导针对被害人的网络暴力乃至现实迫害。为及时保护被害人,《个人信息保护法》第五十七条规定②,平台对已发生的个人信息披露行为应及时补救,包括删除敏感信息、屏蔽禁言等。平台不制止开盒信息散布,应认定为不作为违法。

2.“人肉开盒”行为中“开盒者”民事违法性认定

无论何种模式,开盒者未经被害人同意收集并公布其个人信息的行为均具违法性。“人肉开盒”行为的违法性认定难度源于其特征:单一行为通常仅造成轻微损害,难以从结果层面认定;多主体行为的聚合效应可能引发严重损害,却因侵害者分散而难以从主体层面认定。当封闭主体将受害人信息公布于社交网络却因缺乏网络民意基础受抵制时,其行为未造成严重损害,难以达到规范要求的不法程度;当开放主体基于网络热点事件自发形成人肉搜索侵害受害人时,因主体分散无法追责具体个人,此类轻微违法行为受限于司法成本[8],难以在网络活动中受规制。相反,社工库团体作为网络黑产环节,具有更严重且不可忽视的社会危害性。民事层面,社工库成员以数据库为中心形成紧密团体,未经许可收集、存储、传输并公布个人信息,其违法性显而易见,但民事法律的否定性评价与其社会危害性不相称,需置于刑法领域讨论。

(二)“人肉开盒”行为的刑事违法性认定

民法的私法本质决定其仅具损害填平功能,欲实现对“人肉开盒”行为的犯罪预防,需刑法介入。刑事视域下的违法性讨论,将承继民事违法性认定基础,通过细化与场景化分析,界定罪与非罪、此罪与彼罪的界限。

① 《个人信息保护法》第七十三条第一款:“个人信息处理者,是指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。”

② 《个人信息保护法》第五十七条:“发生或者可能发生个人信息泄露、篡改、丢失的,个人信息处理者应当立即采取补救措施,并通知履行个人信息保护职责的部门和个人。”

1.“人肉开盒”行为中平台刑事违法性认定

平台及其雇员对用户个人信息负有保密义务。向他人非法提供公民个人信息且情节严重的,应以侵犯公民个人信息罪定罪量刑,此系该罪名的常见形态。平台不履行保密义务但未直接侵权的,若雇员非法提供其保有的个人信息,或开盒者获取未加密个人信息且情节严重的,平台构成侵犯公民个人信息罪。不法性层面,平台违反《个人信息保护法》保密义务致个人信息大量泄露,侵害了公民个人信息权益[9];有责性层面,平台对怠于履行保密义务导致的个人信息泄露结果具有预见可能性,却放任结果发生,构成间接故意。需要注意,如果平台不履行其保密义务,经行政机关责令履行后仍不履行,致使个人信息泄露,造成严重后果的,根据《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》(以下简称《解释》)第九条规定,应当以拒不履行信息网络安全管理义务罪定罪处罚。

2.“人肉开盒”行为中“开盒者”刑事违法性认定

刑事视域下开盒者的违法性认定应当聚焦于社工库团队。社工库团队通过对个人信息的非法收集、分发、控制实施侵害,每一个环节都有专门的行为人实施推进,尽管在实践中可能会出现一人“身兼数职”的现象,但理论上仍可区分为“收集者”“分发者”“管理者”三大主体类型。社工库的数据来源多样,包括手段的多样与泄露源的多样。[10]收集者非法的信息收集行为均会触犯侵犯公民个人信息罪,但基于手段与信息来源的不同,其非法收集行为还会额外造成不同的法益侵害,并呈现竞合、牵连等关系。具体而言,“利用受害者的信任、好奇心和贪婪等心理弱点,以冒充熟人或博取同情等社会工程学的方式进行网络盗窃、诈骗和敲诈”[11]获取个人信息,情节严重的,构成侵犯公民个人信息罪,这些行为仅侵害了个人信息持有者的信息权益,而未对计算机信息系统安全、计算机信息系统内存储的数据安全造成损害。若收集者通过网络爬虫爬取以及撞库、注入等黑客手段,未经授权获取公民个人信息,情节严重的,应认定为侵犯公民个人信息罪。此外,其所使用的非法技术手段,还侵犯权利人计算机信息系统的保密性、完整性,[12]未经授权爬取或使用黑客手段获取个人信息,具备获取用于身份认证的个人信息五千条以上的严重情节时,其行为同时触犯侵犯公民个人信息罪与非法获取计算机信息系统数据罪,构成想象竞合。当侵权人为获取个人信息而使用黑客手段破坏计算机信息系统,情节严重时,因其破坏行为与获取行为间呈现手段与目的的牵连关系,而应认定为侵犯公民个人信息罪。

收集到的数据,通过分发者向不特定对象分发的途径,主要有授权社工库访问权限和直接提供社工库内容两种,分发途径的不同影响侵犯公民个人信息数量的认定标准。以提供数据库内容方法分发的,只要分发者向上游非法获取或向下游提供社工库数据,数量满足严重情节的,即构成侵犯公民个人信息罪。以提供权限方式分发的,应根据下游对数据库信息的运用程度进行实质判断。若下游利用该数据库访问权限继续向下分发或利用该数据库全部信息进行模型训练、网络诈骗等活动,应当按照该数据库所包含的全部个人信息数量进行认定;若下游仅对该数据库中部分内容进行利用的,则应以下游利用的个人信息数量进行判断。

社工库团队中,信息收集者与分发者仅是实施有组织犯罪的末端触手,而社工库团队的管理者才是这一组织犯罪的中枢神经。管理者不但指示个人进行信息收集与汇总,还负责招募人员分发社工库信息。管理者与团队成员需要通过通讯网站、群组协同工作,这种设立用于实施社工库活动的网站、通讯群组且情节严重的行为,根据《解释》规定,构成非法利用信息网络罪。此外,管理者作为组织策划、管理社工库团队的首要分子,还应以该团队所犯全部罪行予以处罚。

3.“人肉开盒”行为的刑事违法性认定局限

刑法虽对严重个人信息泄露案件发挥了规制功能,但因规范疏漏,网络犯罪治理仍存困境,受害者保护亦显不足。[7]严重个人信息泄露案件仅是开盒行为的冰山一角。“人肉开盒”行为通常仅侵害极少数自然人信息,与侵犯公民个人信息罪规制的规模化信息泄露行为存在本质区别。对未达数量要件但具显著社会危害性的开盒行为,如何通过规范解释与立法调整实现有效规制,系“人肉开盒”行为规制

的核心难点。

侵犯公民个人信息罪的“严重”“特别严重”情节均难以全面覆盖开盒行为。其一,开盒行为目的多系情绪宣泄而非牟利,故难以通过违法所得入罪;其二,再犯要件难以解决初犯追责困境;其三,开盒行为通常仅针对个别自然人,故数量要件大多情况下难以满足;其四,以“犯罪信息提供”为入罪标准门槛过高,“人肉开盒”行为所附随行为多为违法行为而非犯罪行为。另需注意,开盒者公布被害人信息后,网暴者据此实施违法行为[13],但因开盒者与网暴者无直接关联,二者行为因果关系难以认定。即便因果关系得到确证,网络暴力行为亦难构成犯罪。[14]网络暴力虽难构成侮辱罪或诽谤罪,但负面评论的聚众效应“会营造出当事人被社会主流群体所声讨的局面,使当事人形成身处社会对立面的错觉,也即所谓的‘社会性死亡’”[13]。此类法益损害之严重性毋庸置疑。被害人即便存在道德瑕疵,亦不应适用自我答责理论排除权利保护。[13]

四、法益确证:“人肉开盒”行为法益侵害的双重特征

对开盒行为侵害法益的认识不全面,致使现行刑法难以满足规制需求。基于法秩序统一原则,开盒行为侵害的法益系所有法律、行政法规均需保护的实质性法益。即“所有对于个人的自由发展、基本权利的实现,以及建立在此目标基础上的国家体系的功能运转所必要的现实存在或者目的设定”[15]。该法益保护应依法律后果严重程度分配至各部门法及行政法规。[16]实质性法益构成兼具社会与宪法根据。[16]“人肉开盒”行为侵害的利益是否构成法益需从社会生活层面认定,是否纳入法律保护则需宪法依据。

(一)“人肉开盒”行为所侵害的传统法益内涵

“人肉开盒”行为侵害的传统法益具有多重内涵,被害人个人信息一旦公开即危害其人身与财产安全。《中华人民共和国刑法修正案(七)》增设个人信息犯罪的背景,系非法泄露行为对人身、财产安全和隐私权构成严重威胁。个人信息犯罪立法初衷即包含人身财产安全保护目的,故从形式法益论,该罪保护法益当然涵盖人身与财产安全。虽我国刑法无直接以人身财产安全为保护法益的罪名,但当行为人预备或着手侵害时,仍可通过犯罪停止形态追责予以保护。故人身财产安全始终属刑法保护范畴,可通过具体罪名实现。

开盒者公开被害人信息危害其人身财产安全,通过恐吓造成心理强制及创伤。法国在其刑法典“对人的身心完整性的攻击”一章中将恐吓规定为“威胁罪”,以保护心灵完整性[17];德国刑法则将其归入侵害个人自由罪[18];我国通过寻衅滋事罪行规制,该罪定位于社会管理秩序保护,与“人肉开盒”行为实质侵害的法益存在偏差。开盒恐吓行为实质侵害“心灵完整性”或精神安宁权。神经心理学研究表明,个体遭受社会排斥时的神经活动与遭受身体疼痛时的神经活动具有同质性,一定的社会排斥会导致个体患抑郁症等精神疾病,[19]最终表现为坏情绪乃至抑郁的“躯体化”,甚至导致被害人自残、自杀等严重后果。

精神安宁权与人身、财产安全的宪法依据系“国家尊重和保障人权”与“公民合法私有财产不受侵犯”条款。精神安宁权应纳入人权范畴,既有法国立法例佐证,亦符合我国立法初衷。科学实证显示,精神安宁与身体健康一体两面,身体健康权当然包括精神安宁权。长期的精神压力可诱发精神疾病[20],并损害免疫系统[21],前文提到的社交排斥亦系抑郁症的诱因。[22]这为“人肉开盒”行为会导致抑郁症及自杀倾向的结果①,提供了科学依据。

(二)“人肉开盒”行为所侵害的信息法益内涵

“人肉开盒”行为所侵害的信息法益包括信息安全与个人信息自决权。信息安全包括静态安全与动态安全,前者为信息保密性[23]、完整性[24]、可用性安全[25],后者为信息供给、流通、使用等环节安全[26]。

① 公安部.公安部公布打击黑客犯罪十大典型案例[EB/OL].(2024-09-14)[2025-04-07].http://www.mps.gov.cn/n2254536/n2254544/n2254552/n9309244/n9309283/c9312129/content.html.

非法获取保密个人信息的行为,属于非法获取型数据犯罪,既破坏静态安全中保密性,又侵害动态安全各环节。信息安全法益的入罪基础源于《中华人民共和国宪法》的两条规定:一是“保护非公有制经济合法权益”,二是“保障国有经济巩固发展”。数据在商业运行中至关重要,侵害数据安全将损害经济主体的数据衍生利益,需刑法予以回应。

“人肉开盒”行为通过侵犯个人信息自决权间接侵害传统法益。尽管该权利在法益侵害中工具性显著,但其独立价值不容忽视。信息自决权的宪法基础通常源于人权条款[27]、通信自由与秘密权条款[28]以及人格尊严权条款[29]。学界普遍共识为人格尊严说,即,“个人信息保护指向的是对个体‘数字人格’的保护,……以保护个人自治和个人主体性为内容的人格尊严条款作为个人信息权的基础,应无争议”[30]。该权利衍生于人格尊严权的现实基础在于:网络时代自然人将现实人格投射至网络形成数字人格,其尊严体现为对个人信息的自主处分。“宪法规定人格尊严,……使个人得以在身体与精神上皆免于强制与压迫”[31]。人格网络化背景下,宪法保护的社会生活范畴应延伸至网络虚拟空间。为保障个人精神自由免于强制压迫,确立个人信息自决权系宪法层面的必然要求。

五、规范重构:“人肉开盒”行为的民刑一体化治理

厘清“人肉开盒”行为违法性认定中的规制困境及侵害法益,为民刑共治视野下建构“人肉开盒”行为具体制度奠定基础,通过规范重构以纾解解释论无法应对的治理困境,方可实现对“人肉开盒”行为的合理、全面约束。

(一)民事视域下“人肉开盒”行为的危害预防与消解

民事层面的制度构建通过控制“人肉开盒”行为的产生条件及次生损害范围,实现损害的预防、减轻或阻断。具体方法包括强化个人信息主体的删除权,并引入网络遗忘权制度。

1. 强化个人信息删除权以预防信息泄露

欧盟《一般数据保护条例》(GDPR)规定,当数据与处理目的无关、控制者无保存理由或主体拒绝被处理时,主体可要求收集其信息的企业或个人及第三方删除其信息。我国《网络安全法》第四十三条与《个人信息保护法》第十九条、四十七条确立了处理者的删除义务。具体包括四种情形:处理目的不再必要、保存期满、个人撤回同意、违法违约处理。在此类情形下,处理者需主动履行删除义务,个人亦可行使删除请求权。信息删除权旨在当“以信息自决权为基础建构的‘知情同意’原则(也)出现异化,无法对个人提供有效保护”[32]时,通过限制信息控制者对个人信息的存储利用,控制“人肉开盒”行为产生条件。较之 GDPR,我国个人信息删除制度适用场景较窄,需扩大删除义务范围。以推荐性国标《信息安全技术——个人信息安全规范(GB/T 35273-2020)》为基础,扩展其适用范围以涵盖更多删除场景系可行路径。信息删除权旨在实现服务全面性与信息最小化的平衡。国标分级删除方案通过区分基础/扩展服务的授权与删除,有效限制了处理者信息获取范围,保障部分授权撤销后的基础功能使用。但作为应对,应用会以此为由限制用户使用主要功能,迫使用户维持扩展服务授权或禁止撤回授权。为保障用户充分行使个人信息删除权,应将各功能所需信息范围严格限定于必要范围,实现模块化精细化授权与删除,为用户实现个人信息自决权提供便利。

2. 构建网络遗忘制度预防次生性损害

网络遗忘制度通过控制事件与被害人信息在互联网中的曝光程度与频数,促使互联网参与者被动遗忘,使热点事件被害人逐渐淡出公众视野,从而限制网络传播的负面效应,减轻被害人的网络暴露损害。网络遗忘制度不要求彻底删除信息,而是通过降低公众关注度,使事件逐渐淡出公共视野,实现相对遗忘。社会层面的遗忘以“信息非主动传播”为核心,在网络时代,应限制事件与信息的主动呈现,使热点进入遗忘状态。当个体遭受“人肉开盒”行为或网络暴力时,网络平台、自媒体及论坛应通过算法限制对该话题的推送,约束低创且不全面的报道,降低该事件关注度。此时,算法中立原则应为个人权益保护让

步[33],以平衡网络遗忘权与言论自由的冲突[34]。需认识到,单靠制度无法完全避免损失。一旦“人肉开盒”行为及其次生损害发生时,被害人损失便不可避免。此时法律只能尽量降低行为发生概率并控制损害范围。

(二)刑事领域下“人肉开盒”行为的追责标准再划定

刑事规制旨在通过立法论填补解释论无法保障的法益,具体落实为对精神安宁权、人身及财产安全的保护。具体路径包括:重构恐吓行为规范内涵、区分“公开”与“提供”行为分别入罪、确立“网络暴力”规范标准。

1.重构恐吓行为规范内涵

“人肉开盒”行为可纳入恐吓行为范畴。恐吓系“对他人制造伤害、损害或采取特定行为之意图的表示”。[35]现行刑法对“人肉开盒”行为的恐吓性存在规制缺陷,需单独审视规制。“人肉开盒”行为与寻衅滋事罪的恐吓行为定性相符,属“软暴力”。[36]刑法寻衅滋事罪条文与《关于办理寻衅滋事刑事案件适用法律若干问题的解释》(以下简称《寻衅滋事解释》),已为“人肉开盒”行为入罪提供实践标准,但基于侵害法益属性,将之纳入侵犯公民个人信息罪规制更为妥当。定量层面,依刑法谦抑性,“人肉开盒”行为威胁的利益应限于与被害人密切相关的人身及重大财产权益,且需使被害人感知恐吓可能性,否则难以严重侵害精神安宁权。就“人肉开盒”行为而言,仅公开自然人一般信息(姓名、年龄、身份证号)不足入罪,需叠加公开敏感信息且限制浏览转发量,但开盒者或他人明示将据此实施侵害的除外。参照前述规定,恐吓性开盒行为入罪表述宜为:“在互联网公开可识别特定个人的一般及敏感个人信息,恐吓他人且情节恶劣的行为”。情节恶劣包括:(1)多次(三次以上)恐吓或致他人多次被恐吓,严重影响工作生活;(2)对弱势群体(老人、未成年人、残疾人等)实施前项行为;(3)引发精神失常或自杀等严重后果。

2.区分公开与提供行为

区分公开与提供行为并另行设定入罪标准是另一可行方案。虽然《解释》第三条将公开行为解释为“提供公民个人信息”,但其与一般提供行为并不等同。公开行为具有更高的社会危害性:其一,一般提供行为以牟利为导向,所涉信息多用于商业活动、数据分析或网络诈骗;而具有公开属性的“人肉开盒”行为则以侵害被害人人格尊严、身心健康为目的。其二,一般提供行为的信息流转限于提供者、接收者及次级传播者之间,传播范围可控;而公开行为中,信息传播范围与持续时间均不可控,致个人信息曝光度显著提升。其三,一般提供行为旨在为信息处理提供基础资料,所涉信息均系实现处理目的之必需;而“人肉开盒”行为公开的信息通常涵盖被害人全部可获个人信息,其数据量与敏感度均远超本罪一般提供行为。相较一般提供行为,“人肉开盒”行为的公开属性使其社会危害性显著提高。故《解释》第五条将二者混同的做法,难以准确评价公开行为的危害程度。并非所有“人肉开盒”行为均具入罪所需的恐吓性,但均具有公开性特征。公开行为的入罪标准应独立设定,依信息敏感程度分级。对高度敏感信息,为保护人身财产安全,可参照提供行为标准降低入罪门槛,符合轻罪时代“严而不厉”的结构要求。[37]具体标准可设定为:(1)行踪轨迹、通信内容、征信信息、财产信息等高度敏感信息,十条以上;(2)住宿信息、通信记录、健康生理信息、交易信息等一般敏感信息,五十条以上;(3)其他个人信息,一百条以上。达到上述标准者,应以侵犯公民个人信息罪定罪量刑。

3.确立网络暴力规范标准

“人肉开盒”行为虽属网络暴力范畴[15],但具有独立特性。其通过披露网络使用者现实身份,使网络暴力实施更有效。《解释》通过第五条第一款第(一)(二)项将提供用于犯罪的个人信息行为归入犯罪,规制了披露他人个人信息并引发或助力犯罪的行为。但以“犯罪”为标准存在入罪门槛过高之弊,若改为“违法行为”标准亦不可行:公开个人信息必然招致违法侵害,此标准无法发挥筛选功能,反致标准虚置。以网络暴力为入罪门槛更具合理性。可在《解释》第五条第一款第(一)(二)项基础上,将明知或应知他人正遭网络暴力仍公开其个人信息的行为入罪。该标准依据有三:其一,网络暴力属持续状态,表现为被害

人同时遭受多次违法侵害,精神安宁乃至人身健康安全受侵,其以多次违法为前提,具更高入罪门槛;其二,要求公开行为对网络暴力具加剧作用;其三,网络暴力对被害人法益侵害严重,以其为入罪门槛可发挥限定功能。综上,该标准能在刑事处罚与法益保障间实现平衡,实现对"人肉开盒"行为的全面规制。

六、结语

"人肉开盒"行为是互联网时代的社会必然产物。伴随互联网发展,虚拟网络与物理现实的联结愈发紧密,导致虚拟与现实相互混淆,相互渗透,加剧用户个人信息的泄露风险。辩证地看,自发人肉搜索曾以朴素方式发挥网络监督功能,其初衷是对违背特定行为准则者施以"惩罚",确具积极意义。对能唤起公众同仇敌忾情绪的行为实施人肉搜索,本质是公众通过"人肉开盒"行为及网络暴力对违反社会规范(含强制性规范)的私力救济。这一救济模式既难以通过比例原则划定合理边界,亦无法仅凭法律实现全面治理。作为网络共生的社会现象,法律非唯一治理方式,仅能对"人肉开盒"行为区分规制:对恶意行为实施绝对规制,对具私力救济属性的采取相对规制。

参考文献:

[1] 陈秋心."人肉搜索"语义嬗变:基于雷蒙斯·威廉斯"关键词"方法的探讨[J].现代传播,2023(9):36-45.

[2] 劳东燕.个人信息法律保护体系的基本目标与归责机制[J].政法论坛,2021(6):3-17.

[3] 李建军,刘会强."人肉搜索"与网络传播伦理[J].当代传播,2009(3):72-75.

[4] CLARE H. Affective solidarity:Feminist reflexivity and political transformation[J]. Feminist theory,2012(2):147-161.

[5] 苏宇.网络爬虫的行政法规制[J].政法论坛,2021(6):41-53.

[6] 满涛.网络黑产供给链的结构特征与治理模式[J].学术论坛,2021(3):67-76.

[7] 刘艳红.网络暴力治理的法治化转型及立法体系建构[J].法学研究,2023(5):79-95.

[8] 于龙刚.基层社会的轻微违法行为及其治理路径——基于数地考察的实证研究[J].山东大学学报(哲学社会科学版),2020(6):9-15.

[9] 欧阳本祺.侵犯公民个人信息罪的法益重构:从私法权利回归公法权利[J].比较法研究,2021(3):55-68.

[10] 黄莉莉,徐立稷,黄磊,严梦嘉.社工库信息泄露事件对加强数据安全防护的启示[J].通信企业管理,2023(4):52-53.

[11] 刘权,李东格.网络黑产:从暗涌到奔流[J].互联网经济,2018(6):12-15.

[12] 陈毅坚,曾宪哲.网络爬虫刑法规制研究[J].广东社会科学,2022(5):240-253.

[13] 罗翔,张慧敏.网络暴力治理视域下侮辱、诽谤罪的同质化评价与选择性适用[J].江淮论坛,2023(5):118-126.

[14] 付玉明,刘昕帅.行为解构与危险溯源:"网络暴力"的刑事治理[J].四川大学学报(哲学社会科学版),2023(6):170-179+196-197.

[15] ROXIN C. Strafrecht Allgemeiner Teil,Band I,4 Aufl[M]. München:C. H. Beck,2006:16-19.

[16] 张明楷.论实质的法益概念——对法益概念的立法批判机能的肯定[J].法学家,2021(1):80-96+194-194.

[17] 法国新刑法典[M].罗洁珍,译.北京:中国法制出版社,2003:402-403.

[18] 徐久生.德国刑法典[M].北京:北京大学出版社,2019:210-212.

[19] MACDONALD G, LEARY M. Why does social exclusion hurt? The relationship between social and physical pain[J]. Psychological bulletin,2005(2):202-223.

[20] YAO B, CHENG Y, WANG Z Q, et al. DNA N6-methyladenine is dynamically regulated in the mouse brain following environmental stress[J]. Nature communications,2017(1):8-19.

[21] RUDAK P T, CHOI J, PARKINS K M, et al. Chronic stress physically spares but functionally impairs innate-like invariant T cells[J]. Cell reports,2021(2):35-42.

[22] NIU G F, SUN X J, TIAN Y, et al. Resilience moderates the relationship between ostracism and depression among Chinese adolescents[J]. Personality and individual differences,2016,99:77-82.

[23] 杨志琼.我国数据犯罪的司法困境与出路:以数据安全法益为中心[J].环球法律评论,2019(6):151-171.

[24] 乌尔里希·齐白.全球风险社会与信息社会中的刑法[M].周遵友,江溯,等,译.北京:中国法制出版社,2012:308-310.
[25] 阮晨欣.大数据时代账号注销权的保护实践——以《个人信息保护法》“删除”处理为视角[J].东南法学,2021(2):61-68.
[26] 刘艳红.数据要素全生命周期安全风险的刑事保障制度研究——以数字经济安全法益观为视角[J].法学论坛,2024(1):39-50.
[27] 姚岳绒.论信息自决权作为一项基本权利在我国的证成[J].政治与法律,2012(4):72-83.
[28] 张翔.通信权的宪法释义与审查框架——兼与杜强强、王锴、秦小建教授商榷[J].比较法研究,2021(1):33-48.
[29] 张新宝.论个人信息权益的构造[J].中外法学,2021(5):1144-1166.
[30] 张翔.个人信息权的宪法(学)证成——基于对区分保护论和支配权论的反思[J].环球法律评论,2022(1):53-68.
[31] 张翔.宪法人格尊严的类型化——以民法人格权、个人信息保护为素材[J].中国法律评论,2023(1):57-67.
[32] 万方.隐私政策中的告知同意原则及其异化[J].法律科学(西北政法大学学报),2019(2):61-68.
[33] 赵龙.算法安全法益的理性构造及其规范展开[J].江淮论坛,2023(5):127-135.
[34] 邵国松.“被遗忘的权力”:个人信息保护的新问题及对策[J].南京社会科学,2013(2):104-109+125.
[35] 戴维·M·沃克.牛津法律大辞典[M].李双元,等,译.北京:法律出版社,2003:1103-1104.
[36] 陈灿平,穆亨.新型恐吓行为之刑法规制及扩展分析[J].湖南社会科学,2020(1):39-45.
[37] 刘艳红.犯罪圈均衡化与刑罚轻缓化:轻罪时代我国刑事立法发展方向[J].中国刑事法杂志,2024(1):17-31.

Identification of Illegality of the Acts of “Human Flesh Searching” and “Doxxing” and Their Co-governance Under the Civil Law and the Criminal Law

ZHAO Long, WANG Ziqi

(*Law School*, *Yantai University*, *Yantai*, *Shandong* 264005, *China*)

Abstract: “Human flesh searching” and “doxxing” refer to the acts of collecting personal information via the Internet, compiling it into an identifiable personal profile, and then disseminating it online. This process unfolds in two distinct phases: the “human flesh searching” and the “doxxing”. Currently, the challenges in governance during the “human flesh searching” phase primarily stem from the lack of clarity in assigning responsibilities. Conversely, the “doxxing” phase is fraught with difficulties in effectively preventing harm. At the civil law level, the analysis of the illegality surrounding platform conduct and the actions of those who initiate the doxxing (the “doxxers”) hinges largely on the regulatory stipulations outlined in the *Personal Information Protection Law*. At the criminal law level, the acts of “human flesh searching” and “doxxing”, along with related activities, may constitute offenses such as the infringement of citizens’ personal information, unlawful acquisition of data from computer information systems, and illicit use of information networks. The acts of “human flesh searching” and “doxxing” not only encroach upon the victim’s right to personal information but also pose a threat to their personal and financial security, as well as their mental well-being. To ensure comprehensive safeguarding of legal interests, civil law should incorporate mechanisms to protect citizens’ right to delete personal information and the right to be forgotten online. At the criminal law level, judicial interpretations could be employed to refine the delineation of aggravated circumstances in the crime of infringing upon citizens’ personal information, thereby facilitating the prosecution of offenders and holding them accountable for their actions.

Key words: “human flesh searching” and “doxxing”; crime of infringing on citizens’ personal information; legal interests; co-governance under the civil law and thee criminal law

(责任编辑:董兴佩)