# 大规模侵害个人信息高额罚款研究

孙　莹*

**内容提要**　遏制大规模侵害个人信息是保障自然人个人信息权益、维护公共利益和社会秩序、调整失衡的企业和个人力量、规制互联网竞争生态的需要。对于遏制大规模侵害个人信息，民事追责与刑事定罪均有局限；强化行政执法有必要性，其关键是实施高额罚款。基于贝叶斯纳什均衡等经济分析可知，高额罚款对遏制大规模侵害个人信息是有效的。鉴于欧盟和美国的实践，我国宜对中外企业平等适用高额罚款，以顺应全球个人信息保护的强监管趋势。在现有体制下，赋予网信办实施高额罚款的行政处罚权，并由其负责建立联合执法机制，符合新时代党和国家机构改革面向和依法治国要求。罚款的具体数额应在参考受害人数量、损害大小及侵害公共利益的严重程度等因素基础上，根据大、中、小、微四种不同规模企业的年度平均营业收入进行计算。为保护行政相对人的基本权利，还应规定相应的听证与复议程序。

**关键词**　大规模侵害个人信息　行政执法　高额罚款

DOI:10.14111/j.cnki.zgfx.2020.05.006

随着信息技术的快速发展和互联网应用的普及，数据化、网络化、智能化已经渗透至经济社会的各个方面，不当收集、泄露、利用个人信息的大规模侵权行为也愈加普遍。当今对个人信息的侵害主要以“大规模”为表现形式，例如，以欺诈、诱骗、误导的方式收集个人信息，隐瞒产品或服务所具有的收集个人信息的功能，从非法渠道获取个人信息等大规模不当收集行为；因自身计算机系统缺陷、内部管理不善或第三方原因等导致的大规模泄露行为；滥用个人信息，不当加工个人信息，未经用户同意向第三方传输数据等大规模不当利用行为。本文所称的大规模侵害个人信息指代的是人数众多的不特定的个人信息权益主体因信息处理者同一个行为而遭受侵害的情形。如何增强法律的威慑力以遏制大规模侵害个人信息的发生，值得思考。

## 一、遏制大规模侵害个人信息行为的意义

与普通的个人信息侵权行为相较，大规模侵害个人信息涉及的受害人及信息数量巨大，已经成为个人信息权益受害的主要情形，是我国网络与信息安全领域的一个突出问

* 西南政法大学人工智能法学院副教授，法学博士。

题。遏制大规模侵害个人信息行为，意义重大。

**（一）保障自然人个人信息民事权益的需要**

大规模侵害个人信息的受害人主要为自然人。我国《民法典》第1034条明确规定，自然人的个人信息受法律保护。个人信息既是自然人参与社会交往的载体也是个人人格表现和人格发展的工具，其以对自然人的“可识别性”为核心要素，只能成为自然人权益的客体。对自然人个人信息进行保护，彰显了法律对人格尊严和人格自由的尊重。①

大规模侵害个人信息侵犯了自然人的民事权益并会造成损害，但是此种损害具有不确定性与不可预期性。损害的不确定性不是指个人信息被大规模不当收集、泄露或利用之后是否发生损害不确定，而是指损害的大小、损害的内容、损害何时发生不确定。自然人有可能仅仅是受到微小的损害，也可能因此遭受巨额财产损失甚或严重精神损害。自然人在主动或被动交出个人信息之后，对于信息处理者对个人信息的储存、使用、加工、传输、买卖、提供、公开、修改、删除、销毁等处理活动可能造成的损害无法预期。因为，分散的、琐碎的、表面看来无害的个人信息一旦被汇聚和分析，就可能刻画出我们敏感的、不愿人知的个人信息，对其处理会造成不可预期的后果。而且，造成的损害多为“歧视、身份窃用或诈骗、金融损失、信誉受损、数据泄密、擅自实施的去匿名化以及显著的经济或社会不利后果”等新型损害。② 因此，为保障自然人的个人信息权益，必须遏制大规模侵害个人信息行为。

**（二）维护公共利益和社会秩序的需要**

大规模侵害个人信息侵害了私人利益，同时也侵害了公共利益和社会秩序。正如有学者指出的“个人信息不仅关涉个人利益，而且关涉他人和整个社会利益，个人信息具有公共性和社会性”③，“个人信息衍生出来的社会公共利益，主要是社会治理方面的利益，更不直接归属于个人而为国家或社会所享有”④。这根源于，信息社会是以计算机技术、网络技术、通信技术等为代表的现代信息技术充分扩散和渗透的社会，给社会结构带来最深刻变革，呈现为一种新的社会模式、新的社会形态，其以网络为连接，在社会、生产、生活全领域均有个人信息的处理场景。回溯到社会中的个体，导致在事实上个人信息权益的支配性与排他性相较其他绝对权被弱化，个体的个人信息公共性增强，以个人信息安全为重要内容的信息安全也成为网络安全的核心部分。简言之，在个人信息之上承载了公共信息安全这一公共利益（在经济学语境下可称之为“公共物品”）。

个人信息的公共属性在大规模侵害个人信息场合体现得尤为明显。以对社会秩序的影响为例，信息处理者根据其掌握的海量个人信息，凭借人工智能算法，以用户之间类似的价值观念迅速将单个的用户捏合成有共同诉求的强大团体。在某种意义上，人工智能算法基于个人信息可以为每一个用户赋予特殊性，并将其组织起来，由此在个体碎片

① 参见程啸：《民法典编纂视野下的个人信息保护》，载《中国法学》2019年第4期，第30页。

② 参见叶名怡：《个人信息的侵权法保护》，载《法学研究》2018年第4期，第88-92页。

③ 高富平：《个人信息保护：从个人控制到社会控制》，载《法学研究》2018年第3期，第84页。

④ 张新宝：《〈民法总则〉个人信息保护条文研究》，载《中外法学》2019年第1期，第68页。

化的时代,形成全新政治力量。[⑤] 极端情况下,个人可能被算法操纵从而影响国家政治。“剑桥分析”事件[⑥]即是借助强大的算法模型,利用不当收集的用户信息,造就了一款强大的政治工具来识别摇摆不定的选民,并有针对性地推送可能会产生共鸣的新闻资讯和政治广告,左右选民投票。可以说,在大规模侵害个人信息的场合,个体权利与公共利益、社会秩序及国家安全之间不存在价值平衡的问题,他们的价值具有统一性和一致性。遏制大规模侵害个人信息是维护公共利益和社会秩序及其国家安全的迫切需要。

**(三)调整失衡的企业和个人力量的需要**

由现实来看,大规模侵害个人信息的侵害人主要是企业。新科技革命即现今的信息化进程对社会结构、人类行为、政治权力以及国家关系引发的重大变化,其中之一即是企业拥有着普通人几乎无法逾越的技术壁垒,从而使企业相对个人而言处于了绝对的控制地位,个人丧失了议价空间。企业凭借其资本与日益迭代更新的人工智能及算法,可以更加便捷地实施正当或不正当的信息收集与利用行为。而且,企业的逐利性会力图使个人信息的商业价值性得到最大程度展现。以互联网电商平台为例,结合个人注册信息和浏览偏好,并据此描绘用户的个人特征乃至某类用户群体的社会特征画像,已经成为企业业务的重要组成部分。总之,从信息社会的发展趋势来看,信息技术越发展,其应用越广越深,信息在经济结构中所起作用越大,个人与企业的力量就会越悬殊,加之企业对个人信息规模化利用而逐利的动因,若无国家干预,大规模侵害个人信息行为会越容易发生。因此,在以对大数据挖掘、分析与运用的数字经济时代,为了平衡个人信息权益保护与企业对个人信息的收集利用,就必须要遏制大规模侵害个人信息,调整失衡的企业和个人的力量。

**(四)规制互联网竞争生态的需要**

大规模侵害个人信息破坏了互联网的竞争生态,导致恶性竞争。在互联网经济中,随着人们的追求更加个性化和多元化,各企业不断加强对不同受众群体不同消费观念和习惯的识别,进而实现广告和产品的精准投放。企业如果能够获取更多的个人信息并进行计算识别,可以提高生产效率,降低生产成本,在日益激烈的竞争中获得比较优势。企业的逐利性导致其通过不当途径大规模收集或利用个人信息的意愿增强。但是,这种行为违背了公平竞争原则,如果不对其进行有效遏制,会导致其他企业纷纷仿效,也选择通过不当途径收集或利用个人信息,由此最终导致企业间的恶性竞争,同时出现市场失灵。可见,遏制大规模侵害个人信息,对规制互联网竞争生态有重要意义。

---

⑤ 参见孙莹:《人工智能算法规制的原理与方法》,载《西南政法大学学报》2020年第1期,第85-87页。

⑥ *See* Lesley Fair, *FTC sues Cambridge Analytica for deceptive claims about consumers' personal information*, at https://www.ftc.gov/news-events/blogs/business-blog/2019/07/ftc-sues-cambridge-analytica-deceptive-claims-about(Last visited on Aug.23, 2020).

## 二、高额罚款论的提出与论证

面对大规模侵害个人信息，民法、刑法与行政法各司其职，通过民事追责、刑事定罪与行政执法，追究侵害人的民事、刑事与行政责任。对三种手段遏制大规模侵害个人信息的实效进行全面分析，是本文提出高额罚款论的基础。

### （一）民事追责与刑事定罪的局限

1. 民事追责的局限

由于大规模侵害个人信息侵害了私人利益和公共利益，结合我国《民法典》“总则编”第111条，“人格权编”第1034-1039条，根据“侵权责任编”第1165、1194、1195条的规定，受害人可以提起民事私益诉讼，法律规定的组织也可以提起民事公益诉讼。但是，民事追责具有下述局限性：

其一，大规模侵害个人信息所致损害具有不确定性与不可预期性，导致受害人对损害的存在、种类、范围和程度及损害与行为的因果关系举证困难。⑦ 信息技术的隐秘性决定了信息权益主体难以发现其个人信息在何时何地以及何种程度上被收集和使用。即使《民法典》对个人信息收集利用的规则进行了明确规定，但若信息处理者不予遵守，受害人事实上也难以发现。而且如前述，大规模侵害个人信息所造成的损害通常为新型损害，难以被传统侵权法观念所涵盖，增加了举证难度。

其二，侵权责任法平衡保护受害人的民事权益和行为人的行为自由，基于其事后救济型法律的定位，主要实现的是填补受害人损害的功能，因此，损害赔偿数额也仅以受害人的损失为限，赔偿金额远低于企业实施大规模个人信息侵权行为所获收益。而且，由于传统侵权法对损害要件强调存在“实际经济损失”或“严重精神损害”，受害人受举证责任规则的约束，事实上也难以得到法院支持赔偿的判决。总之，针对大规模侵害个人信息，民事赔偿的功能主要是弥补受害人损失，显然无法对侵害人产生威慑力。

其三，在大规模侵害个人信息场合，产生了“公共物品”之上集体行动难题——“搭便车”困境，且难以解决。集团诉讼，以“为救济大量小额诉讼请求提供充足的动力”为重要目标，以“胜诉酬金制激励律师代表集团成员进行诉讼”为内在驱动，是解决这一困境的良好方案。集团诉讼的启动源于集团拟制，即法院基于代表人申请而作出的集团诉讼确认裁定，禁止退出制和明示退出制均使得法院可以通过裁决将所有潜在的成员纳入拟制的“集团”中。⑧ 在大规模侵害个人信息场合，由于受害人数量巨大，采用集团诉讼来追究侵害人的责任，可使原本处于劣势地位的众多自然人个人因集合而改变诉讼

⑦ 例如在“庞某诉趣拿公司信息泄露案”中，二审判决认为“庞某请求趣拿公司和东航赔偿其精神损失，但现有证据无法证明庞某因此次隐私信息被泄露而引发明显的精神痛苦”。参见北京市第一中级人民法院（2017）京01民终509号民事判决书。

⑧ 参见李激汉：《英美集团诉讼中的特别司法规制及其借鉴意义》，载《法商研究》2017年第2期，第161-165页。

格局，从而能够与侵害人对抗，并对其形成一定程度的威慑。⑨ 我国代表人诉讼与集团诉讼有些许类似之处，但是由于权利人须先登记等技术设计使其运行效果相当不理想。全盘移植集团诉讼制度还是部分引入以改造代表人诉讼，尚需学界进一步讨论并通过人大立法程序将其制度化。⑩ 但是在现阶段，通过集团诉讼追究侵害人的民事责任无制度依据。

其四，大规模侵害个人信息民事公益诉讼运行效果不佳，同时原告还面临着损害赔偿请求权不确定的难题。针对大规模侵害个人信息，可以由消费者权益保护机构或检察机关提起民事公益诉讼。但是整体而言，民事公益诉讼在追究侵害人责任方面发挥的作用尚十分微弱。实践中，消费者权益保护机构提起的个人信息公益诉讼极少，⑪ 检察机关提起的民事公益诉讼数量也远远小于行政公益诉讼的数量。⑫ 尤其需要指出的是，根据《最高人民法院关于审理消费民事公益诉讼案件适用法律若干问题的解释》的规定，未明确原告是否可以要求赔偿损失。就目前来看，否定损害赔偿请求权的声音在学界和司法实务界依然强劲。⑬ 欠缺“损害赔偿请求权”尤其是“惩罚性赔偿请求权”的大规模侵害个人信息民事公益诉讼，显然无法对侵害人产生威慑力。

2. 刑事定罪的局限

刑法是剥夺生命、自由等“最严厉的制裁”的规范，⑭ 因此适用刑法打击大规模侵害个人信息非常必要。大规模侵害个人信息的侵害人主要是企业，其犯罪属于单位犯罪。与之相关的罪名主要是《刑法》第 253 条之一“侵犯公民个人信息罪”和第 286 条之一“拒不履行信息网络安全管理义务罪”，该二罪以涉及个人信息的数量作为入罪标准之一，针对非法获取、出售或者提供的行为，三类个人信息分别达到五十条以上、五百条以上、五千条以上，被视为“情节严重”，数量达到前述标准十倍以上被视为“情节特别严重”；针对拒不履行信息网络安全管理义务致使用户信息泄露的行为，三类个人信息分别达到五百条以上、五千条以上、五万条以上被视为“造成严重后果”。⑮ 可以说，在大规模侵害个人信息的场合，单位犯罪门槛非常低。但是，刑事责任具有下述局限性：

---

⑨ 例如，“Gaos 诉谷歌案”中，原告指控谷歌通过向第三方披露个人信息这一方式来操作其搜索引擎侵犯其互联网隐私权，谷歌最终支付了 850 万美元和解金终结，其中 25% 由法院分配给律师。*See* In re Google Referrer Header Privacy Litig., 87 F. Supp. 3d 1122(2015).

⑩ 参见鄢焱：《中国不宜引入美国式集团诉讼制度论》，载《信阳师范学院学报（哲学社会科学版）》2017 第 6 期，第 50–54 页。

⑪ 能够查阅到的案例仅有一例，即江苏省消费者权益保护委员会对北京百度网讯科技有限公司提起的我国首例个人信息消费民事公益诉讼。由于立案后百度公司积极进行整改，该案以撤诉结案。参见江苏省南京市中级人民法院（2018）苏 01 民初 1 号民事裁定书。

⑫ 参见韩静茹：《公益诉讼领域民事检察权的运行现状及优化路径》，载《当代法学》2020 年第 1 期，第 130 页。

⑬ 参见杜乐其：《消费民事公益诉讼损害赔偿请求权研究》，载《法律科学》2017 年第 6 期，第 168–180 页。

⑭ 参见马克昌：《危险社会与刑法谦抑原则》载《人民检察》2010 年第 3 期，第 8 页。

⑮ 参见《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）第 5 条；《最高人民法院、最高人民检察院关于办理非法利用信息网络、帮助信息网络犯罪活动等刑事案件适用法律若干问题的解释》（法释〔2019〕15 号）第 4 条。

其一，上述二罪制裁的对象只包括非法提供、出售、获取个人信息和拒不履行信息网络安全管理义务致使用户信息传播、泄露的行为，即转移个人信息型行为，对“不当利用”行为，尤其是“合法获取、不当利用”行为缺乏规范，因此，现行刑法对大规模侵害个人信息的打击范围有限。除非不当利用信息行为正好符合其他犯罪构成要件规定，如结合敲诈勒索行为或采用入侵计算机信息系统的形式，否则刑法束手无策。⑯ 根据刑法的补充性、片断性和宽容性等刑法谦抑性理念，对社会关系的调整，民法救济与行政制裁应被优先考虑，刑法是最后的手段，且应限于最小限度领域，并慎重处罚。个人信息是数字经济时代数据生产要素的源头，因此必须平衡个人信息保护与数据利用，⑰ 对个人信息不当利用进行妥当规范。在刑法谦抑性理念之下，对个人信息不当利用能否纳入犯罪圈及其构成要件为何，⑱ 显然需要立法者的深思熟虑。

其二，刑罚趋于轻缓而且罚金数额相对较低，对侵害人威慑力不足。笔者以 2017-2019 年为范围在北大法宝司法案例库进行检索，以案件标题含有“公司”进行筛选，引用《刑法》第 253 条之一和《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》第 7 条判定单位犯“侵犯公民个人信息罪”的裁判文书有 76 份，引用第 286 条之一判定单位犯“拒不履行信息网络安全管理义务罪”的数量为 0。以“侵犯公民个人信息罪”为例，已有的涉及大规模侵害个人信息的刑事定罪判决，仅涉及到了部分大规模侵害个人信息行为类型，尚无有影响力的判决。就刑罚而言，根据刑法规定，单位犯前述罪名的，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规定处罚。但是，实践中，缓刑是刑事责任的主要形式，而且单位犯罪的罚金数额较小。⑲ 此外，存在罚金判定失范化问题，其中大多并无罚金依据的基数和倍数等标准的说明，针对类似行为，不同法院判定的单位罚金数额差异也较大。通过上述实证考察，可以发现：虽然刑事立法上针对大规模不当收集、泄露个人信息行为的入罪门槛极低，但是刑事司法上追究企业等主体的刑事责任之情形并不常见；即使少部分企业及其责任人被刑事定罪，刑罚也较为轻缓。简言之，在大规模侵害个人信息场合，侵害人的刑事责任呈现出“严而不厉”的态势。

**（二）强化行政执法的必要性**

由上可见，民事追责与刑事定罪的局限性导致其对侵害人的威慑力不足。行政法以促进公共利益最大化为基本目标，行政机关作为公共利益的维护者和个人间利益的平衡

⑯ 参见李川：《个人信息犯罪的规制困境与对策完善——从大数据环境下滥用信息问题切入》，载《中国刑事法杂志》，2019 年第 5 期，第 35 页。

⑰ 参见张新宝：《从隐私到个人信息：利益再衡量的理论与制度安排》，载《中国法学》2015 年第 3 期，第 49 页。

⑱ 参见冀洋：《法益自决权与侵犯公民个人信息罪的司法边界》，载《中国法学》2019 年第 4 期，第 66 页。

⑲ 根据笔者统计，对直接负责的主管人员和其他直接责任人员，判处缓刑的有 61 人次，判处短期自由刑的有 20 人次，其中，1 年以下刑期的有 6 人、1 年以上 3 年以下刑期的有 9 人、3 年以上刑期的有 5 人；就单位罚金而言，20 万元以下居多，达到 62 例，20 万元以上仅有 14 例，其中，罚款最少的是 3000 元，罚款最多的是 100 万。

者,需要不断调整其在经济、社会事务中的作用边界和方式。[20] 国家作为提供安全和秩序的“利维坦”,在大规模侵害个人信息行为发生时自然不应缺席。基于行政执法的特性,强化行政执法是遏制大规模侵害个人信息的关键之举。

1. 行政执法可以覆盖的大规模侵害个人信息的行为类型更加全面

个人信息保护是互联网治理的重要内容,从世界范围看,在过去20年间,国家在互联网治理中的力量不断上升,提高对互联网的国家监管力度成为一种全球普遍趋势。[21] 就我国而言,有20余部行政法律法规对行政机关在个人信息权益保障、信息行业发展和法律责任等方面的职权作出了规定,政府通过行政处罚能够施加的监管范围非常广泛,违反个人信息保护义务的行政处罚条款涉及各个具体领域。而且,行政法规范可以较容易实现对不当收集、泄露、利用等全部大规模侵害个人信息行为类型的覆盖。与刑法相比,不限于个人信息转移型侵害行为;与民法相比,不必受限于隐私权和个人信息(权)等概念,调整范围都更广。

2. 行政执法可以及时高效介入大规模侵害个人信息事件

众所周知,行政权执行力强,具有强制性、富有扩展性,对社会具有直接影响力;与司法权相比,行政权是主动、直接对事务进行管理,司法权则被动地解决社会争端。就个人信息保护而言,行政机关掌握更多的个人信息相关技术,具备更为专业的知识和调查能力。在互联网大数据、电子商务和社会信用建设等涉及个人信息保护的领域,我国选择了政府与市场协同发展的模式,政府作为产业政策和国家标准的制定者积极介入其中。因此,行政机关既是个人信息保护领域的政策和行业标准制定者,也是市场监管者,这使其有足够的资源和能力来应对企业的大规模侵害个人信息行为。此外,与司法机关只能就大规模侵害个人信息案件进行个案处置相比,行政机关还可以基于典型的个人信息行政执法案例,制定相应的个人信息保护“公共政策”,从而谋求预防和惩治大规模侵害个人信息的有效策略。

3. 行政执法可以为大规模侵害个人信息的民事追责与刑事定罪提供支撑

民事责任、刑事责任与行政责任绝不是割裂开来的。同一大规模侵害个人信息的行为,给他人造成损害的,依法承担民事责任;违反行政法规范的,依法承担行政责任;构成犯罪的,依法承担刑事责任。就刑事定罪而言,根据我国《刑事诉讼法》第54条第2款规定,“行政机关在行政执法和查办案件过程中收集的物证、书证、视听资料、电子数据等证据材料,在刑事诉讼中可以作为证据使用”,因此,在对大规模侵害个人信息先行实施行政处罚的情况下,可以为检察机关提起侵犯公民个人信息罪等公诉提供有力的证据支撑。就民事追责而言,由于目前众多的个人信息保护规范在性质上是一种公法规范、管制性规范,而违反安全性规范规定的公法上义务,对侵害人是否承担侵权责任具有

[20] 参见沈岿:《行政法变迁与政府重塑、治理转型——以四十年改革开放为背景》,载《中国法律评论》2018年第5期,第74页。

[21] 参见刘建伟:《国家“归来”:自治失灵、安全化与互联网治理》,载《世界经济与政治》2015年第7期,第120页。

直接影响。[22]

### （三）高额罚款论的提出

根据目前行政法律法规的规定，针对大规模侵害个人信息的行为，行政机关享有广泛的行政职权且行政处罚手段多样。除约谈和公开通报外，行政处罚措施还包括责令改正、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、没收违法所得和罚款。这其中，罚款是最重要的手段。[23]

行政罚款是一种财产罚，它是行政主体为了维护公共管理秩序，在行为人违反行政义务而又不构成犯罪时，依法给予的一种经济上的制裁。[24] 与责令改正等行政处罚相比，行政罚款直接触及违法行为人的经济利益，可对从事市场经营活动的行政相对人（尤其是企业）产生直接的制裁作用，因此效果明显。同时，它又不像吊销相关业务许可证等行政处罚剥夺了行政相对人从事特定行业的资格，没有直接剥夺相对人的活动自由，因此效果相对缓和。而且，采用可量化的行政罚款符合行政处罚日益专业化的发展方向。同样是以情节轻重作为判断标准来选择适用其他行政处罚方式，会导致行政机关实施行政处罚的自由裁量权过大，也加大了个案中具体执行的难度。[25] 而相较于其他种类的行政处罚，罚款的优势在于其可量化性，即可以将不同违法情节与不同的罚款金额相对应，较为明确地实现违法行为与处罚的一一对应，从而提高行政处罚的威慑性和精确性。

但是，目前我国行政法律法规对侵害个人信息行为的行政罚款多数采用封顶式，罚款额度各异，最高也未超过 100 万元，[26] 从具体的行政执法实践来看，罚款金额也普遍较低。[27] 与企业因侵权行为可获得的高收益相比，目前的罚款额度根本不足以遏制大规模侵害个人信息行为。如前所述，面对大规模侵害个人信息中企业与个人力量的失衡和企业间竞争生态的破坏，应当重视行政机关对抗“市场失灵”的作用，强化行政执法具有必要性。其中，罚款作为使用频率最高的行政处罚方式有其优势，提高罚款金额增加侵

---

[22] 参见孙莹：《论侵权责任法与安全性规范的关系——以大规模侵权的预防为切入点》，载《西南民族大学学报（人文社会科学版）》2012 年第 8 期，第 83 页。

[23] 笔者在浙江省政务服务网“行政处罚结果信息公开”栏以案件名称中的“个人信息”为查询条件，以 2016 年 1 月—2020 年 3 月为限，可以查询到 332 个行政处罚结果，以此为样本进行梳理发现：从具体的行政处罚方式来看，责令改正的占 28%，警告的占 26%，当场训诫的占 17%，行政拘留的占 5%，没收违法所得的占 4%，罚款的占 73%。参见浙江政务服务网，http://www.zjzwfw.gov.cn/zjzw/punish/frontpunish/showadmins.do?webId=21，2020 年 3 月 25 日访问。

[24] 参见陈太清：《行政罚款与环境损害救济——基于环境法律保障乏力的反思》，载《行政法学研究》2012 年第 3 期，第 58 页。

[25] 例如《网络安全法》第 64 条规定：“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。”据此，行政机关可自由裁量采用何种处罚方式。

[26] 例如，1 万元以上 10 万元以下；2 万元以上 10 万元以下；2 万元以上 20 万元以下；5 万元以上 50 万元以下；10 万元以上 100 万元以下；违法所得 1 倍以上 10 倍以下罚款，没有违法所得的，处 100 万元以下罚款。参见《网络安全法》第 59、64 条；《电子商务法》第 76 条；《征信业管理条例》第 40–42 条。

[27] 仍以笔者在浙江省政务服务网“行政处罚结果信息公开”栏的查询案件为样本所做数据统计为例，从罚款具体数额来看，罚款 1 万元以下的占约 11%，罚款 1 万元的占 16%，罚款 1–2 万元的占 3%，罚款 2 万元的占 22%，罚款 3 万元的占 8%，罚款 5 万元的占 2%，罚款 10 万元的占 3%，罚款 20 万元、30 万元的均占 1.5%。参见浙江政务服务网，http://www.zjzwfw.gov.cn/zjzw/punish/frontpunish/showadmins.do?webId=21，2020 年 3 月 25 日访问。

害人的违法成本是强化行政执法的应有之义和必然要求，也具有天然的正当性。基于此，本文提出大规模侵害个人信息高额罚款论，即提高现行法律针对大规模侵害个人信息的行政罚款金额，同时使罚款金额不受受害人实际损失或侵害人违法所得的限制，具体实施方案详见后文论述。

**（四）高额罚款的经济学分析**

经济学认为，每一个从事经济活动的人所采取的经济行为都是力图以自己最小经济代价去获得最大的经济利益。同时，罚款的确定性与严厉性与侵害者的违法代价密切相关，并直接影响侵害者遵守法律的意向。因此，笔者尝试从经济学视角，基于“成本—收益”原理和贝叶斯纳什均衡，就加强行政执法实施高额罚款对遏制大规模侵害个人信息的有效性进行分析。

1. 两种处罚模式对侵害人与行政机关的影响

假设有权行政机关对大规模侵害个人信息的侵害人处以罚款有两种选择：罚款数额巨大或罚款数额较小。两种处罚模式分别会对行政机关（国家）、侵害人产生不同的影响。

首先，对侵害人而言，其是否顾忌行政处罚，取决于行政处罚导致其所花费的成本是否大于其侵害个人信息所获得的收益。如果罚款数额较小即违法成本低，特别是在侵害人所获得的收益大于罚款数额时，侵害人的占优战略是实施违法行为，因此结果是：罚款数额较小不仅不能产生阻却侵害人实施违法行为的后果，而且还将进一步助长侵害人实施更多违法行为。反之，侵害人的占优战略则是不再实施违法行为。其次，对行政机关（国家）而言，当罚款数额较小时，得到罚款，损失因个人信息保护执法损耗的行政资源即执法成本；就行政执法效果而言，特别在侵害人所获得利益大于罚款数额而进一步实施违法行为时，会导致受害人受到损害且对社会信任感降低。当罚款数额巨大时，得到罚款，同样损失执法成本；就行政执法效果而言，特别是在侵害人所获得收益小于罚款数额时而停止实施违法行为时，会使受害人避免损害且对社会信任感上升。

在实践中，个人信息侵害人往往更加关注自身违法行为所导致的自身的资源损耗即违法成本。因此，以阻却违法者的行为为目的，最直截了当的做法，就是大幅提升其违法之后的行政罚款金额，使其违法成本相应提高，尤其应使违法者的收益小于违法成本，为整个动态博弈场域树立起相对静止的标准，以此强化对侵害人的影响。

2. 个人信息侵害人视角下的不完全信息博弈

从个人信息侵害人的视角看，其无法判断行政机关的资源损耗的数值。行政资源损耗的数值是不确定性条件下的选择问题，侵害人不仅不知行政资源损耗的数值是高还是低，更无法知晓不同个人信息侵害类型之下的行政资源损耗的分布概率。

在对博弈过程进行论证之前，要说明的是，面对侵害人可能作出的大规模侵害个人信息的行为，行政机关执法的行政资源损耗可能较低，也可能较高；当侵害人实施违法行为时，有权行政机关可能对其进行处罚，也可能不处罚。侵害人在评估其行动战略时，应考虑两个因素：行政罚款的金额和行政机关进行处罚的概率。具体从侵害人视角而

言，行政罚款的金额越高，侵害人的违法意愿越低；同时，行政处罚的概率主要取决于执法成本，如果行政机关的执法成本很高，处罚侵害人的概率会降低；如果执法成本在行政机关可承受的范围内，则处罚侵害人的概率会提高。

（1）行政罚款金额对侵害人的影响

假设在实施侵害个人信息的行为之后，侵害人不被处罚所获得利益是1亿元，被处罚将额外损失2500万元，在侵害人对行政机关的执法成本不了解的情况下，侵害人可以预估行政机关对其不处罚的概率为P(Z)，则处罚的概率为1−P(Z)。侵害人的期望收益可以被计算为：1亿元 ×P(Z)+（−0.25亿元）×[1− P(Z)]，设平均期望收益为0，则P(Z) = 0.2，则1− P(Z)=0.8。如果不被处罚所获得利益数额不变，被处罚额外损失5000万元，则P(Z) ≈ 0.33，1− P(Z) ≈ 0.67；额外损失为7000万元时，P(Z) ≈ 0.4，1− P(Z) ≈ 0.6；额外损失为1亿元时，P(Z)= 1− P(Z)=0.5。

由上可见，随着罚款金额的提高，特别是大幅提升行政罚款金额，使侵害人所获得的收益小于违法成本，即便在被处罚的概率下降的情况下，仍能促使侵害人作出不再实施违法行为的战略选择。简言之，缩小不被处罚所获得收益与被处罚所受损失的差距，可以强化对侵害人的影响。与此同时，侵害人必然还将对行政机关的行政资源损耗成本进行预估，以帮助判断其被处罚的概率。

（2）侵害人对行政机关执法成本高低概率的预估

基于前述，本文运用贝叶斯纳什均衡理论演释侵害人在信息不透明的动态环境中如何基于动态的不完全的信息（多轮博弈）来推导行政机关的高执法成本概率，力图展示侵害人根据对行政资源损耗的预估，进而对其违法行为是否会被处罚作出评估并对是否实施违法行为作出战略选择的过程。

本文假设，侵害人预估行政机关为高执法成本的概率为60%，低执法成本的概率为40%；高执法成本之下侵害人被处罚的概率为20%，低处罚成本之下侵害人被处罚的概率为100%。

a. 首轮博弈：根据假设，侵害人所受处罚概率的预估值为0.6×0.2+0.4×1 = 0.52。在首轮博弈后，侵害人从所受处罚概率的预估值可以推断出行政机关为高执法成本的概率为(0.6×0.2)÷0.52 ≈ 0.21<0.6。此时侵害人认为行政机关属于高执法成本的概率就从0.6转为0.21，低执法成本的概率则从0.4转为0.79。b. 第二轮博弈：侵害人所受处罚概率为0.21×0.2+0.79×1 = 0.83。此时侵害人从所受处罚概率的预估值可以推断出行政机关的高执法成本概率为（0.21×0.2）÷0.83 = 0.05。c. 通过两轮博弈可见，侵害人认为行政机关属于高执法成本的概率从0.6到0.21再到0.05，因此侵害人作为理性的市场经济主体，当行政机关对其不断作出行政处罚时，会降低侵害人认为行政机关属于高执法成本类型的概率，从而使侵害人拒斥违法行为。

综上，可以得出结论，在经济学的逻辑中，若对大规模侵害个人信息处以罚款太少，远远低于其违法所得，将会进一步助长违法行为，导致大规模侵害个人信息的案件频繁发生；而加强执法频次且对大规模侵害个人信息实施高额罚款，则可以从根本上有助于

促使信息处理者或控制者采取措施积极履行法律责任，进而构建“激励相容的个人数据治理体系”㉘。

## 三、对欧盟和美国高额罚款实施机制与实践的考察

从世界范围来看，欧盟和美国的个人信息保护水平处于前列，是世界各国构建个人信息保护法律制度的重要参考范例。同时，我国与欧盟、美国相似，互联网通讯行业亦处于全球领先地位，个人信息保护问题也愈加突出，且所管辖地域幅员辽阔，个人信息保护的执法机构众多而分散，面临着如何协调各地区执法机构关系的问题。因此研究大规模侵害个人信息的高额罚款问题，不能忽略欧盟和美国在个人信息保护领域的实践。

### （一）对欧盟高额罚款实施机制与实践的考察

2018年5月25日，欧盟《通用数据保护条例》（以下简称GDPR）正式生效。㉙ GDPR整合成员国国内的独立数据保护机构，并强化此类机构在跨境案件中的合作，以及在欧洲数据保护委员会（European Data Protection Board，以下简称EDPB）的内部合作，建立了创新的治理体系。㉚ 伴随着引领世界个人信息保护法发展潮流的雄心，欧盟将其个人信息行政处罚权力大大扩张至欧盟之外，隐约搭建起了国际空间的个人信息执法霸权。

#### 1.SA和LSA的法律地位与职责

欧盟个人信息保护行政监管执法体制的基石，实际上是立足于各成员国的独立监管机构（Supervisory Authority，以下简称SA）。GDPR授权各成员国设立一个或多个SA，负责监督GDPR在成员国的实施。各成员国还可以依规定选定领导性监管机构（Lead Supervisory Authority，以下简称LSA），以协调多个SA的合作并统一处理数据控制者和处理者的跨境问题。㉛ 当一个成员国确立了不止一个监管机构，该成员国应当在EDPB委任一个监管机构代表其他机构，并建立一致性机制涵盖其他机构而与欧盟委员会进行合作。

GDPR明确了SA的独立地位。GDPR第52条第1款和第2款规定，各成员国设立的SA具有独立的法律地位，在执行职权时不受外部影响。第52条第4款规定，成员国应当提供必要条件，保障SA履行行政监管职责，包括必需的人力性、技术性与资金资源，前提性与基础性要素，选择和雇佣其成员的权力等。第57条第1款第f项规定，SA可

---

㉘ 周汉华：《探索激励相容的个人数据治理之道——中国个人信息保护法的立法方向》，载《法学研究》2018年第2期，第3页。

㉙ *See Regulation (EU) 2016/679 of the European Parliament and of the Council*, at https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1598321477138&uri=CELEX:32016R0679(Last visited on Aug.23, 2020).

㉚ *See Data Protection as a Pillar of Citizens' Empowerment and the EU's Approach to the Digital Transition - Two Years of Application of the General Data Protection Regulation*, at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020SC0115(Last visited on Aug.23, 2020).

㉛ GDPR第56条第1款规定：“在不影响第55条的前提下，控制者或者处理者的主要营业机构或唯一营业机构所在地的监管机构应当可以充当领导性监管机构，监管控制者或处理者根据第60条程序而进行的跨境处理。”

以受理信息主体或实体、组织或协会根据 GDPR 第 80 条的申诉，有权调查申诉的主要内容。根据 GDPR 第 58 条的规定，SA（包括 LSA）享有调查权力[32]、矫正性权力[33]、授权和建议性权力[34]三大类权力。另外根据 GDPR 第 83 条第 2 款的规定，SA 和 LSA 实施行政罚款的权力既可以是其他矫正性权力的补充，也可以成为其他矫正性权力的替代措施。另外，第 60 条第 1 款规定，LSA 与其他 SA 应当建立信息共享和合作机制。

2.SA 和 LSA 的合作与争议解决机制与 EDPB 监管之下的纠纷解决机制

就不同监管机构间的合作与争议解决机制，GDPR 第七章作出了规定。其中包括两种情况：LSA 和其他 SA 的合作；SA 之间的合作。

就 LSA 和其他相关 SA 的合作，GDPR 第 60 条规定，LSA 在 GDPR 规定的职权范围内可以要求 SA 提供必要的互助合作，而且可以根据第 62 条而进行联合行动。此外，LSA 和其他相关 SA 也存在平等性合作关系，例如，在处理涉数据控制者和处理者的跨境问题时，LSA 应当听取相关 SA 的意见，具体步骤如下：（1）LSA 将处理的事项通知相关的 SA，并充分考虑其他 SA 的意见，及时向其他 SA 提交一份决定草案。（2）如果其他 SA 在四周内提出了草案的合理反对意见，若 LSA 同意该反对意见，则应当在两周内将一份修订后的草案决定提交给其他 SA。若 LSA 不同意该反对意见，则应当将该争议事项提交给第 63 条规定的一致性机制。

就 SA 之间的合作，GDPR 第 61 条规定了各 SA 之间的互相协助。SA 应当为彼此提供信息和互相协助，以便以统一的方式执行和适用 GDPR，并在其之下进行有效的相互合作。对于某个 SA 的请求，其他 SA 都应当在一个月之内及时回应，而且应当视情况告知为了实现请求而采取的措施。被请求的 SA 如果拒绝，应当提供说明。超过一个月仍不提供相关信息的，做出请求的SA可以在其成员国境内采取三个月以内的临时性措施。

GDPR 也规定了 EDPB 监管之下的纠纷解决机制。GDPR 第 65 条规定了 EDPB 在处理不同 LSA、SA 间处理意见分歧可以采取的措施。当相关 SA 对 LSA 的草案决定提出合理反对或 LSA 驳回其反对时，EDPB 就以裁决者的身份出现，对该问题作出具有约束力的最终决定。作出此类决定的期限为一个月，若主体事项较为复杂，可以再延长一个月。当 EDPB 无法作出决定，其应当以 EDPB 理事会成员简单多数的方式，在第二个

---

[32] 调查权力具体包括：要求控制者和处理者等提供履行其任务所需要的所有信息；以数据保护核查的方式进行调查；对根据 GDPR 所颁布的认证进行审查；将可能侵犯 GDPR 的情况告知控制者或处理者；从控制者和处理者那里获取访问个人数据，以及为了行使监管任务而所需的所有信息的权力；按照欧盟与成员国法律的程序法，获取对控制者和处理者所有房屋建筑及场地，包括数据处理设施和方法的访问权。

[33] 矫正性权力具体包括：对控制者或处理者予以警告；当处理操作侵犯 GDPR 条款的时候，对其进行申诫；命令其尊重数据主体行使符合 GDPR 的权利；命令其处理操作符合 GDPR 条款；命令将个人数据泄露的情况告知数据主体；对处理施加暂时性或具有明确期限的禁令；要求对个人数据进行纠正或擦除等；撤回认证等；视每个案例的情形不同，还可施加行政罚款；要求中止将数据传输到第三国或国际组织。

[34] 授权和建议性权力具体包括：根据提前咨询条款向控制者提出建议；主动或根据要求为全国性议会、成员国政府提供意见，或者根据成员国法为其他机构、实体与公众提供和个人数据保护相关的保护；如果成员国的法律要求此类提前咨询，依授权处理；发布意见以及行为准则；委任认证机构；颁发认证和批准认证的标准；制定数据保护标准条款；授权有关合同条款；授权有关行政行安排；批准约束性公司规则。

月的期限结束后的两周内作出决定。如果EDPB成员的投票刚好完全分裂,那么将根据主席的投票而作出决定。

3. 欧盟高额罚款的实践

欧盟各成员国的数据保护机构已经平衡使用了其强化的矫正性权力,包括警告和谴责、罚款和临时或最终处理限制。在2018年5月25日至2019年11月30日期间,22个欧盟/欧洲经济区数据保护机构实施了大约785笔罚款。[35] 罚款数额总额以英国、意大利、法国、德国居多,处罚的行为涵盖了技术和组织措施不足、无法确保信息安全,不遵守一般数据处理原则,数据泄露通知义务的履行不充分等11种类型。[36] 尽管全面评估新的合作与一致性机制的功能还为时过早,但数据保护当局通过一站式执法机制和大量使用互助手段建立了合作关系。

以英国及其对英航公司的处罚为例,根据GDPR第51条的规定,英国设立信息专员办公室(Information Commissioner's Office,以下简称ICO)作为其独立的国家性数据监管执法机构。ICO不隶属于既有的行政机构,直接对国会负责。2018年6月起英国航空公司(British Airways)网站发生数据泄露事件,导致近50万名英航乘客的个人信息遭泄露。虽然受害人来自不同欧盟国家,各国数据监管机构均有权行使管辖权,但根据GDPR第56条关于LSA职权的规定,最终由ICO作为LSA代表其他欧盟国家的数据监管机构进行调查,并对英国航空公司作出拟罚款1.839亿英镑的通知。[37]

**(二)对美国高额罚款实施机制与实践的考察**

美国的个人信息保护依循的是隐私保护路径。由于种种原因,美国联邦贸易委员会(Federal Trade Commission, 以下简称FTC)成为美国信息隐私方面最广泛、最具影响力的调节力量。[38] 其最初是为了确保商业竞争的公平,后职权不断扩大,最终成为事实上的联邦数据保护机构。FTC对侵犯隐私权案件行使管辖权的基本法律依据是《联邦贸易委员会法》第5(a)条,即它禁止"不公平或欺骗性的行为存在或者影响商业"[39],执法部门是消费者保护局。FTC对美国国内跨州、各州与国外的涉及公共利益(消费者权益保护和公平竞争)的商业案件享有广泛的行政调查权、执法权和立法权,这也使其在调查大型企业,尤其是跨国企业的个人信息侵权问题上有明显的优势。在其执法活动中,

---

[35] *See Data Protection as a Pillar of Citizens' Empowerment and the EU's Approach to the Digital Transition - Two Years of Application of the General Data Protection Regulation*, *supra* note 30.

[36] *See* Fines Statistics, at https://www.enforcementtracker.com/?insights(Last visited on Aug.23, 2020).

[37] *See Intention to Fine British Airways £183.39m under GDPR for Data Breach*, at https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/ico-announces-intention-to-fine-british-airways/(Last visited on Aug.23, 2020).

[38] *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, Columbia Law Review, Vol.114, p.585(2014).

[39] *A Brief Overview of Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority*, at https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority(Last visited on Aug.23, 2020).

采取高额的罚款日益成为越来越重要的执法手段。[40] 例如，FTC 几乎可以不受限制地自行决定“同意令的程序和范围”，包括经济处罚、禁止特定活动和采取纠正措施，通常还包含长达 20 年的报告、审计和合规性要求。[41]

2019 年 7 月，FTC 宣布与 Facebook 达成一项创纪录的 50 亿美元和解协议。此前，Facebook 被指控通过欺骗性隐私设置侵害个人的信息隐私而违反了 2012 年 FTC 的隐私令，联邦法院法官于 2020 年 4 月 23 日签署命令批准了该协议。[42] 本案的罚款数额虽然非常高，但是仍有一些方面值得我们注意。

第一，即使该罚款占 Facebook 2018 年收入的 9%，但由于该和解协议放弃了对 Facebook 隐私保护问题的“结构性解决方案”，该协议实际上无法有效遏制 Facebook 对用户信息的侵犯。市场将之解读为“用罚款换宽松监管”，在和解协议公布的当天，Facebook 的市值不跌反涨，收盘时上涨 100 亿美元。这提醒我们，对于那些在市场占据头部地位的超大型企业，除了巨额罚款外，执法机构还应当针对具体情况设置其他有效的监管措施，避免超大型互联网公司期望的“以罚代管”的现象发生。

第二，FTC 选择与 Facebook 达成和解协议的原因之一在于，如果选择诉讼会消耗大量的资源，得到结果不一定比和解协议更为理想。可见，即使是 FTC 这种联邦级执法机构在处理案件中也对可能的巨额执法成本有所担忧。这提醒我们，未来我国的执法机构在调查超大型互联网公司的大规模侵害个人信息行为时同样可能面临较高调查成本的问题，这种成本是省级以下的执法机构所无法承担的。所以，针对超大型互联网企业的调查和执法权宜由国家一级的执法机构享有。

第三，尽管本案的罚款金额空前，但这种罚款比例并非我国在制定高额罚款时所能借鉴的标准，原因在于：其一，美国有所谓辩诉交易传统，为减少诉讼成本，政府针对许多大企业的商业调查都以附高额罚款的和解方式结案。这种方式虽然减少政府的诉讼成本，但客观上一定程度以放松对企业的强监管为代价。其二，GDPR 的颁布标志着欧盟在个人信息保护领域成为全球的领先者并产生了“布鲁塞尔效应”，其在隐私权保护原则、范围、执法权等方面甚至会影响美国互联网行业和相关政府部门的政策制定，美国正试图积极应对这一局面，[43] 并意图在个人信息保护领域与欧盟展开竞争。这就导致 Facebook 案中的高额罚款不免带有某种宣示色彩，其意图表明美国在个人信息保护领域

---

[40] 以 2019 年为例，2 月，短视频应用 Musical.ly 因违反美国《儿童在线隐私保护法》（以下简称 COPPA）而被 FTC 处以 570 万美元罚款；7 月，FTC、美国司法部宣布与 Facebook 达成和解，对 Facebook 开出 50 亿美元的罚单；9 月，Equifax 公司同意与 FTC、消费者金融保护局以及美国 50 个州和地区达成和解，被处罚款 5.75 亿美元；9 月，谷歌旗下视频分享网站 YouTube 因非法收集和分享儿童个人信息，违反 COPPA 而被罚款 1.7 亿美元。*See* FTC, *Privacy & Data Security Update: 2019*, at https://www.ftc.gov/reports/privacy-data-security-update-2019(Last visited on Aug.23, 2020).

[41] *See* Daniel J. Solove&Woodrow Hartzog, *supra* note 38, p.613-614.

[42] *See* United States *v*. Facebook, Inc., No. 1:19-cv-02184 (D.D.C. July 24, 2019), at https://www.ftc.gov/system/files/documents/cases/182_3109_facebook_order_filed_7-24-19.pdf (Last visited on Aug.23,2020).

[43] *See* Rustad, Michael L. & Koenig Thomas H, *Towards a Global Data Privacy Standard*, Florida Law Review Forum, Vol. 71, p.365-454(2019).

同样可以与欧盟旗鼓相当,甚至更为激进。而这两方面均非我国在制定高额罚款时主要考虑的问题,因而本案也难以成为我国执法机构在实施行政处罚时的参考范例。

## 四、我国实施高额罚款的具体方案

与欧盟及美国相较,我国目前缺乏统一的个人信息保护行政监管执法机构并赋予该机构以必要的法定职权,导致罚款裁量基准体系不系统与裁量肆意,从而削弱了执法力度与效果。本文在借鉴域外有益经验基础上,根据我国的实际提出以下具体方案。

### (一)赋予网信办实施高额罚款的行政处罚权

我国当前针对个人信息保护的行政监管执法权分散在工信、公安、商务、人民银行、工商行政管理、发改委等不同国家机关和部门当中,多头监管导致难以形成监管合力。而由于大规模侵害个人信息案件的技术性强、涉案人员众多且案件频发,因此需要一个专业机构负责处理。除网信办外,以上各行政机构在面对这一新兴的侵权案件时均可能能力不足,既有的职责与相互关系使得它们难以迅速互相协调。网信办作为其中新设立的机构,执行对大规模侵害个人信息的调查与处理具有有利条件。网信办职责虽然广泛,但是目前的法律或行政法规并未赋予其明确的行政处罚权,导致其在查处网络违法案件中只能进行约谈,或依靠其他拥有行政执法权的部门进行处罚。因此,为了解决目前大规模侵害个人信息案件中执法力量分散、执法机构职责交叉的问题,建议考虑赋予网信办高额罚款的行政处罚权,并由网信办负责建立联合执法机制。

其一,赋予网信办高额罚款的行政处罚权,符合新时代党和国家机构改革朝向国家治理现代化的目标。2018 年 3 月中共中央印发的《深化党和国家机构改革方案》(以下简称《方案》)指出,在新的历史起点上深化党和国家机构改革,以国家治理体系和治理能力现代化为导向,以推进党和国家机构职能优化协同高效为着力点,改革机构设置,优化职能配置。深化党和国家机构改革具有问题导向性,即着力解决一些领域突出存在的党政机构重叠、职责交叉、权责脱节问题。因此,需要对既有的不适应新时代中国社会主义发展和国家治理现代化的行政体制、机构和职能设置进行调整。赋予网信办行政处罚执法权,一定程度上可改变目前国务院现行网络信息安全管理体制。实际上,为维护互联网健康发展,并维护国家网络空间安全,国家已经逐步赋予网信办更多的职权。在行政机构改革中, 2011 年 5 月,国务院办公厅发出通知设立国家互联网信息办公室,但当时网信办不另设新的机构,只是在国务院新闻办公室加挂网信办的牌子。至 2014 年,根据《国务院关于授权国家互联网信息办公室负责互联网信息内容管理工作的通知》(国发〔2014〕33 号),国务院明确授权国家网信办负责全国互联网信息内容管理工作,并负责监督管理执法。同年,在党的机构改革中,中央网络安全和信息化领导小组成立。2018 年,根据《方案》,将中央网络安全和信息化领导小组改为中央网络安全和信息化委员会,其办事机构为中央网络安全和信息化委员会办公室,同时,将国家计算机网络与信息安全管理中心由工信部管理调整为由中央网络安全和信息化委员会办公室管理,这

表明党对互联网安全的重视达到了新的高度。同年,为了推进提高党政机构的决策和运行效率,将国家网信办与国家互联网信息办公室这两个职能相近的党政机构合署办公。而根据《国务院关于机构设置的通知》(国发〔2018〕6号),国家互联网信息办公室与中央网络安全和信息化委员会办公室是一个机构两块牌子,列入中共中央直属机构序列。由此可见,网信办在国家互联网治理中被赋予越来越重要的位置,因此适合被授予高额罚款的行政处罚权。

其二,赋予网信办高额罚款的行政处罚权符合依法治国的要求。社会主义法治必须坚持党的领导,党的领导必须依靠社会主义法治。党在加强国家网络信息安全体制建设过程符合社会主义法治要求。2018年2月,党的十九届三中全会通过了《中共中央关于深化党和国家机构改革的决定》和《方案》。2018年3月,为贯彻《方案》,国务院向第十三届全国人民代表大会第一次会议提请审议《国务院机构改革方案》并获通过,为国务院机构改革提供了合法性基础。此外,依照《宪法》和《国务院组织法》,国务院也有权授权网信办行使高额行政处罚执法权。《宪法》第89条规定,国务院的职权包括"规定各部和各委员会的任务和职责,统一领导各部和各委员会的工作,并且领导不属于各部和各委员会的全国性的行政工作"。《国务院组织法》第11条规定,国务院可以根据工作需要和精简的原则,设立若干直属机构主管各项专门业务,设立若干办事机构协助总理办理专门事项。此外,现行的法律法规,如《网络安全法》《儿童个人信息网络保护规定》等,也规定了网信办有权采取相应的执法行动,证明了其作为网络安全执法机构的地位,同时也为网信办行使行政执法权提供了依据。

关于网信办的职权行使,本文建议如下:第一,在大规模侵害个人信息案件中赋予网信办高额罚款行政处罚权,并不意味着网信办在所有涉互联网安全领域享有统一执法权,尤其在其他互联网安全执法领域,网信办的职责主要是在联合执法中起统一协调作用。由于各部委、各机构对个人信息保护的侧重点不尽一致,职权上也有相互重合之处,易在行政监管执法实践中出现摩擦,而网信办可以利用其职责的灵活性,负责建立与工信部、市场监督管理局、商务部等的联合执法机制,因此建议将我国有权机构的个人信息保护行政执法权,由国家网信办统一负责协调。第二,考虑到大规模侵害个人信息案件在审查中要求行政机关具有很强的专业性,其行政处罚的金额较大甚至巨大,为保障执法的有效性和科学性,并保障相对人的合法权益,本文建议将大规模侵害个人信息案件的管辖权限定在国家网信办和各省级网信办。对具体案件的管辖权可综合参考侵权企业规模、受害人数加以划分。例如可以规定涉案的微型和小型企业,且受害人数不足5000人的案件,由省级网信办管辖;如果涉案的是中型企业和大型企业,或受害人数达5000人以上的案件,由国家网信办管辖。另外,由于大规模侵害个人信息的受害人很可能分布在不同区域,因此可能出现不同省级网信办对同一案件均享有管辖权的情况。对此,为了提高行政效率,可以由先立案的省级网信办统一处理,如果两个以上的省级网信办同时立案,或后立案的网信办对此提出异议,则由国家网信办进行管辖权裁定。

### （二）高额罚款的参考因素

我国《行政处罚法》第 4 条规定，设定行政处罚必须以事实为依据，与违法行为的事实、性质、情节以及社会危害程度相当。大规模侵害个人信息高额罚款作为一种行政处罚，也应遵循合理行政原则，即在进行罚款金额的设定时应考虑到罚款的有效性、成比例性和劝诫性。有效性指罚款应当切实得到实行，成比例性指个案的罚款金额应当结合主体种类、行为和情节加以确定，劝诫性指罚款金额应当足以警告和惩罚违法主体的违法行为。

但是，目前我国对大规模侵害个人信息的行政处罚条款，没能将罚款的有效性、成比例性和劝诫性这三个原则转化为具体可量化的规定，因此削弱了行政罚款的优势。GDPR 第 83 条第 2 款同时从客观层面、主观层面和造成损害结果方面出发，规定了作出行政处罚的诸多参考因素，[44] 在参考因素基础之上构建了高额罚款制度，并于第 83 条第 4、5、6 款规定了三种情况下不同的罚款额度。对此，我们可以予以借鉴。考虑到成文法难以事无巨细地规定大规模侵害个人信息的全部行为类型，通常会规定有权行政机关在处理案件时可以行使自由裁量权，此时，比例原则有着重要的遵循意义，它一方面要求有权行政机关规范自身实施的行政处罚，另一方面也为法院在行政诉讼中审查有权行政机关行政处罚的合理性提供标准。因此，结合大规模侵害个人信息的特征，对其实施高额罚款应当考虑以下要素：第一，受害人数量多少。根据受害人人数的多少认定侵权情节的严重性。为了尽可能实现对个人信息的保护目标，受害人达到 100 人以上可视为受害人人数较多，受害人达到 500 人及以上可定义为受害人人数众多，受害人达到 5000 人及以上可定义为受害人人数特别众多。第二，对受害人造成的损害的大小。由于大规模侵害个人信息所致损害具有不确定性与不可预期性，其发生还具有隐蔽性，因此应尽可能细化其考量因素，具体应包括受害人经济损失和精神损害、侵权企业的违法所得等因素。第三，侵害的公共利益的严重程度。如前所述，大规模侵害个人信息案件会造成公共利益和社会秩序的破坏，因此，在具体个案中应考虑案件波及的领域和影响的程度。总之，在大规模侵害个人信息案件中，适用比例原则实施高额罚款，是对侵害人施加有效而不过度的行政处罚，可确保个案公正。

### （三）高额罚款的计算标准

2019 年，德国数据保护监管机构（Datenschutzkonferenz）（以下简称 DSK）基于 GDPR 第 83 条设计了罚款的计算模式，并发布了《关于确定企业 GDPR 相关罚款数额的官方指

---

[44] 参考因素具体包括：结合相关处理的性质、范围或目的，被影响的信息主体的数量以及损害程度而确定的违法的性质、严重性与持续时间；违法的性质是基于故意还是过失；个人信息控制者或处理者为了减轻信息主体损失而采取的所有行动；结合控制者或处理者采取的符合 GDPR 的技术性与组织性措施而认定的控制者或处理者的责任程度；控制者或处理者之前的所有相关违法行为；为了纠正违法行为和减轻违法所造成的可能负面影响而和监管机构进行合作的程度；为违法行为所影响的个人信息类型；监管机构得知违法行为的方式，特别是控制者或处理者是否对违法行为进行了报告，以及在何种程度上进行了报告；如果对同一主题事项已经对控制者或处理者发布 GDPR 规定的措施，对这些措施是否遵守；遵守已生效的行为准则或认证机制；对于案件情形可以适用的所有加重或减轻因素，例如因为违法而直接或间接导致的经济收益、避免的损失。

南》。该计算模式已经在德国被运用，并且可能将使高额罚款成为常态。欧盟为了统一执法实践，EDPB 可能在欧洲范围内采取此种罚款模式。[45] 对于罚款的标准和步骤，为确保制裁有效、成比例性和劝诫性，该指南以不同种类企业的营业额作为标准，并规定了 5 个步骤以确定具体罚款数额。[46] 结合我国的情况，本文试对我国针对大规模侵害个人信息高额罚款的数额判定步骤作以下说明：

步骤一，区分企业规模大小。可以根据 2017 年国家统计局发布的《统计上大中小微型企业划分办法》中对信息技术服务业中的大、中、小、微企业（下文表格分别用字母 D、C、B、A 指代）的营业数额进行划分。[47]（见表 1）

**表 1　大中小微企业的营业数额划分**

| | | | | | | |
|---|---|---|---|---|---|---|
| A. 年度营业收入在 50 万元以下 | B. 年度营业收入在 50 万至 1000 万元 | | C. 年度营业收入在 1000 万至 1 亿元 | | D. 年度营业收入超过 1 亿元 | |
| | B. Ⅰ | 年度营业收入 50 万至 100 万 | C. Ⅰ | 年度营业收入 1000 万元至 3000 万元 | D. Ⅰ | 年度营业收入 1 亿至 2 亿 |
| | B. Ⅱ | 年度营业收入 100 万至 500 万元 | C. Ⅱ | 年度营业收入 3000 万元至 5000 万元 | D. Ⅱ | 年度营业收入 2 亿至 3 亿元 |
| | B. Ⅲ | 年度营业收入 500 万元至 750 万元 | C. Ⅲ | 年度营业收入 5000 万元至 7500 万元 | D. Ⅲ | 年度营业收入 3 亿元至 4 亿元 |
| | B. Ⅳ | 年度营业收入 750 万元至 1000 万元 | C. Ⅳ | 年度营业收入 7500 万元至 1 亿元 | D. Ⅳ | 年度营业收入超过 4 亿元 |

步骤二，确定不同规模企业的平均年度营业收入。[48] 这一步骤是为了阐明在此基础上确定的步骤三中的罚款基数，具体计算以表 1 为基础。（见表 2）

---

[45] *See* Tim Wybitul, *German DPAs push model for higher GDPR fines*, at https://iapp.org/news/a/german-dpas-push-model-for-higher-gdpr-fines/(Last visited on Aug.23, 2020).

[46] Vgl. Konzept der DSK zur Bußgeldzumessung in Verfahren gegen Unternehmen, URL: https://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSKBeschluessePositionspapiere/Okt19_Konzept_Bu%C3%9Fgeldbemessung.html(abgerufen am 23.Aug, 2020).

[47] 此处需要说明的是，为适应我国国情，本文对企业规模采取四分法。另外，2017 年《统计上大中小微型企业划分办法》按照行业划分，并对不同行业中大中小微企业的划分标准各有不同，为了论述的方便，本文仅选择信息技术服务业这个最可能发生大规模侵害个人信息行为的行业加以讨论，但不影响对其他行业也采取同样的分析方法。

[48] 此处需要说明的是，平均年度营业收入并非取两年的平均收入，而是将下限与上限相加取其平均数，目的是为了确定同一规模企业的平均年度营业收入。例如，营业收入在750万元至1000万元之间的企业，不同企业营业收入仍有不同，但法律无法为其一一确定罚款基数，为公平起见，只能取其平均数作为罚款基数。只要企业属于该规模内，无论其营业收入是低于或高于 875 万元，均按照 875 万元计算。另外，具体的年度营业收入以企业实施侵权行为而遭行政处罚的前一年的年度营业收入为标准。

表 2 不同规模企业的平均年度营业收入

| | | | | | | |
|---|---|---|---|---|---|---|
| A.25 万元 | B. Ⅰ | 75 万元 | C. Ⅰ | 2000 万元 | D. Ⅰ | 1.5 亿元 |
| | B. Ⅱ | 300 万元 | C. Ⅱ | 4000 万元 | D. Ⅱ | 2.5 亿元 |
| | B. Ⅲ | 625 万元 | C. Ⅲ | 6250 万元 | D. Ⅲ | 3.5 亿元 |
| | B. Ⅳ | 875 万元 | C. Ⅳ | 8750 万元 | D. Ⅳ | 实际营业收入 |

步骤三,核定罚款基数。罚款基数是将各类别企业的平均年度营业收入除以 360( 天 ) 得到的四舍五入成整数的每日罚款金额 ( 见表 3 )。其中,对年度营业收入 4 亿以上的企业进行罚款的最高限额为其实际年度营业收入的 2%–4%,即罚款根据各企业的实际营业收入计算。

表 3 核定罚款基数

| | | | | | | |
|---|---|---|---|---|---|---|
| A.694 元 | B. Ⅰ | 2083 元 | C. Ⅰ | 55556 元 | D. Ⅰ | 416667 元 |
| | B. Ⅱ | 8333 元 | C. Ⅱ | 111111 元 | D. Ⅱ | 694444 元 |
| | B. Ⅲ | 17361 元 | C. Ⅲ | 173611 元 | D. Ⅲ | 972222 元 |
| | B. Ⅳ | 24306 元 | C. Ⅳ | 243056 元 | D. Ⅳ | 不超过实际年度营业收入的 2%–4% |

步骤四,依据违法行为严重程度明确因数,乘以罚款基数。根据个案中违法行为的具体情况,本文将行为的严重程度分为轻度、中度、严重和非常严重。在本步骤中,根据现行法律的规定并考虑个案情形,按照表 4 确定违法行为严重程度及其对应的因数,将因数与罚款基数相乘。以本文伊始列举的大规模不当收集个人信息的行为类型为例,可选择的与之对应的不同的因数如下。( 见表 4 )

表 4 违法行为严重程度及相应的罚款因数

| 行为严重程度 | 以欺诈、诱骗、误导的方式收集个人信息 | 隐瞒产品或服务所具有的收集个人信息的功能 | 从非法渠道获取个人信息 |
|---|---|---|---|
| 轻度 | 1 至 2 | 1 至 2 | 1 至 4 |
| 中度 | 2 至 4 | 2 至 4 | 4 至 8 |
| 严重 | 4 至 6 | 4 至 6 | 8 至 12 |
| 非常严重 | 大于 6 | 大于 6 | 大于 12 |

步骤五,依其他情形对罚款数额进行调整。根据所有在步骤四中未曾考虑的对企业有利或不利的情形,对依据步骤三、四所计算出的罚款金额进行调整。在此需要考虑的情形包括违法行为的整体情形以及其他情形,例如企业是否积极弥补漏洞、及时通知大规模侵犯个人信息的受害者等。

### （四）高额罚款的听证、复议程序

为保护行政相对人的基本权利，本文认为，在确立大规模侵害个人信息高额罚款制度中，也应当规定相应的听证程序，并提供相应的复议程序保障。

1. 行政听证程序

如前文所述，针对大规模侵害个人信息的罚款金额较大甚至巨大，基于依法行政的原则，根据《行政处罚法》第 42 条关于“行政机关作出责令停产停业、吊销许可证或者执照、较大数额罚款等行政处罚决定之前，应当告知当事人有要求举行听证的权利；当事人要求听证的，行政机关应当组织听证”的规定，拥有行政执法权的网信办应当为接受行政处罚的行政相对人提供必要的听证程序。

《行政处罚法》第 42 条对于听证程序作出了基本规定，但涉及到处理大规模侵害个人信息的行政处罚这一新问题时，有两方面仍值得注意。第一，大规模侵害个人信息的行政处罚听证程序是否需要公开。根据《行政处罚法》第 42 条第 1 款第 3 项规定，“除涉及国家秘密、商业秘密或者个人隐私外，听证公开举行”。由于大规模侵害个人信息行为往往涉及大量的自然人信息，笔者建议不予公开。第二，大规模侵害个人信息案件的听证对于行政机关和相对人在互联网行业了解方面有更高的专业要求。从行政机关角度来看，长期以来存在的听证主持人资格不明确和素质不高等问题可能进一步显现，因此有必要加强网信办的专业人才队伍建设，并考虑设立专门的听证主持人。从行政相对人的角度看，行政相对人一方可能既需要当事人本人出席，也需要一名技术人员或专家提供专业知识，如果回应学界呼吁的明确律师参与权，相对人一方可能需要三人出席。但《行政处罚法》第 42 条第 1 款第 5 项规定，“当事人可以亲自参加听证，也可以委托一至二人代理”，这意味行政相对人一方最多只能有两人出席。因此，如何在遵守《行政处罚法》的同时为相对人提供充分的发表观点的机会仍值得思考。

2. 行政复议程序

如前文所述，大规模侵害个人信息行政处罚案件应由国家和省级网信办管辖。相应的，在具体案件的行政复议中，其复议机关各不相同。根据《行政复议法》第 12 条规定，“对县级以上地方各级人民政府工作部门的具体行政行为不服的，由申请人选择，可以向该部门的本级人民政府申请行政复议，也可以向上一级主管部门申请行政复议”。因此，对于省级网信办作出行政处罚的案件，其复议机关为省级人民政府或国家网信办。而根据《行政复议法》第 14 条规定“对国务院部门或者省、自治区、直辖市人民政府的具体行政行为不服的，向作出该具体行政行为的国务院部门或者省、自治区、直辖市人民政府申请行政复议。”因此，对于国家网信办作出行政处罚的案件，其复议机关为国家网信办。行政复议申请人也可以向国务院申请裁决，国务院依照《行政复议法》的规定作出最终裁决。

## 结 语

信息社会的个人信息保护事关每个个体的福祉。综合运用各类法律责任，提高法律威慑力，遏制大规模侵害个人信息的发生，意义重大。需要说明的是，本文倡导高额罚款论，但绝不否认民事赔偿与刑事制裁的作用，也绝不否认罚款以外的行政处罚手段的作用。以我国《个人信息保护法》的起草为契机，本文提出，就当前大规模侵害个人信息的遏制，当务之急是解决侵害人违法与侵权的低成本问题，关键之举是强化行政执法，其核心是实施高额罚款，目的是对侵害人形成更强的威慑力。由省级以上网信办对企业实施的大规模侵害个人信息行为作出行政处罚，罚款金额以不同类型企业的平均年度营业收入为标准，并参考侵权行为的危害程度综合计算得出。通过提高现行法的罚款金额，增加了侵害人的违法成本，能够对其形成较强的威慑力。同时，高额罚款平等适用于实施大规模侵害个人信息的中外企业，尤其是在中国境内从事互联网行业的大型跨国公司，以顺应全球个人信息保护的强监管趋势。

**Abstract:** Curbing large-scale infringement of personal information is the need to protect the rights and interests of natural persons' personal information, adjust the unbalanced corporate and individual power, safeguard public interests and social order, and regulate competitive ecology of the Internet. There are limitations in civil accountability and criminal conviction for curbing the large-scale infringement upon personal information. It is necessary to strengthen administrative law enforcement, the core of which is to impose high fines. Based on economic analysis such as Bayesian Nash equilibrium, high fines are effective in curbing large-scale infringement of personal information. In view of the practice of EU and US, China should equally apply high fines to Chinese and foreign enterprises in order to comply with the global trend of strong supervision of personal information protection. Under the current system, the Cyberspace Administration of China is given the administrative power to impose high fines and is responsible for establishing a joint law enforcement mechanism, which is in line with the reform orientation of Party and state institutions in the new era and the requirements of rule of law. The specific amount of fines shall be calculated according to the annual average operating income of large, medium, small and micro enterprises of different sizes on the basis of factors such as the number of victims, the extent of damage and the severity of the infringement of public interests. In order to protect the fundamental rights of administrative counterparts, corresponding hearing and reconsideration procedures should also be stipulated.

（责任编辑：任 彦）