个人信息的侵权法保护

叶名怡*

内容提要：一切个人信息均属侵权法的保护范围，对非敏感个人信息提供侵权法保护不会阻碍信息流通。侵权法对个人信息提供两种保护路径，即侵权责任法第36条的网络信息侵权条款及其司法解释，以及同法第6条过错侵权条款配合民法总则第111条。个人信息侵权各项构成要件应适当缓和，如承认若干新型损害、建立三元归责原则体系、复数控制人场合设立因果关系推定等。在个人信息侵权救济方面，重视更正、停止处理、删除、数字加密等预防性责任方式的运用。关于金钱赔偿，应在（过失）帮助侵权、不确定因果关系等场合下新增连带责任规定，并将安保义务及其被违反所导致的补充责任予以扩张，以适用于作为虚拟场所管理人的数据存储者。在泛实名制的背景下，我国应选择更接近于欧洲的信息保护模式而非美国模式。

关键词：个人信息　侵权法　构成要件　预防性责任　责任形态

民法总则第111条规定，“自然人的个人信息受法律保护”，这是我国民法首次明确规定保护个人信息。侵权法是民事权益保护的一般性法律，其保护哪些个人信息，具体应如何保护，信息侵权的构成要件和法律效果有何独特之处，这些新问题尚未获得充分讨论和回应。本文对此展开研究。

一、保护范围与保护路径

（一）保护范围

从民法总则第111条的文义来看，自然人的一切个人信息均受民法保护，没有例外。有学者认为，个人信息数量众多，其边界过于模糊，“个人外界无法识别且捉摸不定，无法为他人行为划定禁区”。〔1〕不过，现行法和司法解释对于个人信息的范围进行了明确界定。

全国人大常委会2012年颁布的《关于加强网络信息保护的决定》第1条规定：“国家

* 上海财经大学教授。

〔1〕 参见杨芳：《个人信息自决权理论及其检讨——兼论个人信息保护法之保护客体》，《比较法研究》2015年第6期，第33页。

保护能够识别公民个人身份和涉及公民个人隐私的电子信息。”此处采取的是“定义 + 列举式”规定，即法律保护隐私信息和（其他）个人信息。个人信息的本质在于其可识别性。

2017 年 6 月 1 日起施行的《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，下称“信息刑案解释”）第 1 条规定，“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。”此处采取的同样是“定义 + 列举式”规定。个人信息具可识别性，其范围同样包括隐私信息和一般信息。

2014 年 10 月 10 日起施行的《最高人民法院关于审理利用信息网络侵害人身权益民事纠纷案件适用法律若干问题的规定》（法释〔2014〕11 号，下称“信息侵权解释”）第 12 条规定：“网络用户或者网络服务提供者利用网络公开自然人基因信息、病历资料、健康检查资料、犯罪记录、家庭住址、私人活动等个人隐私和其他个人信息，造成他人损害，被侵权人请求其承担侵权责任的，人民法院应予支持。”此处是“列举 + 兜底式”规定，个人信息的范围同样包括隐私信息和一般信息。

由上述现行法和司法解释可知，个人信息的范围界限基本上清楚明确，侵权法既保护隐私信息（敏感信息），〔2〕也保护不属于隐私的一般信息。而且，从比民法刚性更强的刑法视角来看，信息主体之外的其他人的“行为禁区”也是清晰的，“信息刑案解释”除了第 1 条（个人信息界定）和第 13 条（施行日期之规定）外，其他 11 个条文都是关于定罪、量刑的具体规定，都是在为他人划定清晰的“行为禁区”。举重以明轻，刑法上侵害个人权益的禁止性行为，在民法（侵权法）上也属于禁止性行为。

连“不重要的”非隐私信息都给予保护，是否过犹不及？肯定者认为，如此全面的信息保护会导向严格的信息限制甚至是信息禁止，〔3〕从而“在价值上对私人自由构成无端干涉”。〔4〕其实这种担忧是不必要的，因为按照德国法理论通说和审判实践，信息主体对其信息所享有的权益属于一般人格权。〔5〕作为一般人格权的信息权益，其行使与保护有自身强烈的独特性，详述如下：

第一，人格权的支配性与支配权的支配性有本质差异。拉伦茨在论述权利的概念和分类时指出：权利是法律赋予主体的一种“法律的力”，但“‘法律的力’不适用于各种人格权，法律没有规定主体对人身的‘权力’”，“各种人格权都是与人结合在一起的，不可移转，也不可继承”；而支配权意味着权利人可对“‘他的物’随意处分，原则上可以随意放弃或转让，还可以继承”。〔6〕可见，与支配权全方位的利用和处置权能不同，人格权主要

〔2〕 自 2018 年 5 月 1 日起实施的推荐性国家标准《信息安全技术——个人信息安全规范》（GB/T 35273 - 2017）第 3.2 条对个人敏感信息作如下界定：“一旦泄露、非法提供或滥用可能危害人身和财产安全，导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息。”从其定义看，敏感信息与隐私信息的外延大体相当。

〔3〕 参见杨芳：《我国个人信息保护法适用范围之思考——隐私权救济困境下的个人信息保护法》，《社会科学家》2016 年第 10 期，第 113 页。

〔4〕 参见杨芳：《德国一般人格权中的隐私保护——信息自由原则下对“自决”观念的限制》，《东方法学》2016 年第 6 期，第 116 页。

〔5〕 Staudinger/Hager (2017), C. Das Persönlichkeitsrecht, Rn. C173, Rn. B140.

〔6〕 ［德］卡尔·拉伦茨：《德国民法通论》上册，王晓晔等译，法律出版社 2013 年版，第 276 页，第 286 页。

体现为一种消极性的防御权,〔7〕权利人能够对人格要素具有的支配权能极其有限。信息主体对个人信息的支配主要体现为信息的使用（自己使用），主旨在于维护自身人格的自由发展。至于收益权能（许可他人使用），其实是个人信息属性中的财产属性的应用，并非信息人格权的固有内涵。信息主体对个人信息几乎不享有什么处分权能，信息人格权益既不可移转也不可继承。因此，信息不是物，信息主体对个人信息不享有无限制的任意支配权，全面的信息保护不会造成信息主体对信息的恣意支配。

第二，人格权的排他性与支配权的排他性也有重大不同。支配权“是一种全面的排他性的权利，根据这种权利，一切他人都不得对此物施加影响”；而人格权本质上“是一种受尊重权，即承认并且不侵害人所固有的‘尊严’，以及人的身体和精神，人的存在和应然的存在”。〔8〕可见，与支配权的排他性服务于其强大的支配效力不同，人格权的排他性主旨在于获得他人尊重，亦即，只有当外界的介入损害到主体尊严时，这种排他性才会发挥作用。就此而言，个人信息被他人收集或使用，只要在一般观念上没有损害到信息主体尊严，即不构成对后者权益的侵犯。事实上，依据欧盟《一般数据保护条例》（General Data Protection Regulation，下称《数据条例》）第6条，获得信息主体同意仅仅是“合法处理数据”的六种法定依据之一。可见，信息主体对个人信息所能享有的排他性是非常弱的。全面保护个人信息不会引发信息交流停滞。

第三，个人信息的侵权判定原则上要进行利益衡量。在判定人格权侵权是否成立时，或者说在判定处理他人信息的行为是否违法时，利益衡量必不可少。〔9〕梅迪库斯指出，“一般人格权的主要问题在于它的不确定性，因为对一个人的保护，往往是以牺牲另一个人的权利或利益为代价的。因此在发生争议时，必须进行利益衡量。”〔10〕这种特定意义上的利益衡量在物权等其他领域并不存在，而只存在于一般人格权领域（德国将名誉权、隐私权也纳入一般人格权）。因此，若将信息主体对信息的利益界定为一般人格权，那么，在判断个人信息是否被侵害时，就应当进行利益衡量，即比较信息主体的信息利益与信息收集者或处理者对信息处理所具有的其他利益，只有当前者大于后者时，才可以禁止信息处理。更一般地说，对个人信息一般性地提供保护与具体场景下提供保护不是一回事。在具体场景下，应否保护个人信息并拒绝他人使用，须个案综合判断，并不能从“一般性地全面保护个人信息”直接推导出“书写或呼叫他人姓名即侵犯他人信息权益”这样的极端结论。保护范围的宽广性与保护要件设定的严格程度，是可以分离也应当分离的两个问题。

当然，信息敏感度不同，法律保护力度亦不同。对隐私信息（敏感信息）和一般信息作区别对待是比较法上的通例，如欧盟《数据条例》第9条、2018年5月25日生效的最新德国联邦数据保护法（BDSG，下称“德国数据法”）第46条第14款、我国台湾个人资料保护法（2015）第6条等等。个人信息敏感度的划分源于隐私领域的分类。德国法中的领域理论将私领域分为诸如家庭住址、电话号码等一般私人领域（Privatsphaere），诸如书信、

〔7〕 王泽鉴：《人格权法》，北京大学出版社2013年版，第277页。

〔8〕 前引〔6〕，拉伦茨书，第282页，第284页。

〔9〕［德］汉斯·布洛克斯、［德］沃尔夫·瓦尔克：《德国民法总论》，张艳译，中国人民大学出版社2012年版，第426页。

〔10〕［德］迪特尔·梅迪库斯：《德国民法总论》，邵建东译，法律出版社2013年版，第807页。

通话内容等秘密领域（Geheimssphaere），以及诸如性活动等隐秘领域（Intimsphaere）。〔11〕尽管王泽鉴指出，“人口普查案”弃用领域理论，改以数据的使用或结合可能性作为判定标准，〔12〕但该案判决书的原文是，“信息在何种程度上是敏感的，并不仅仅（nicht allein）取决于其是否涉及隐秘经历”。〔13〕可见，德国法院并未一般性地抛弃领域理论，而只是对其作增补以应对自动化数据处理场合下数据画像带来的威胁。有人认为，“并不存在绝对受到保护的、无需利益衡量即可推定出侵害行为违法性的核心领域（即隐秘领域）。”〔14〕然而，隐秘领域如性领域应尽可能予以保护，按德国通说甚至应绝对受保护。〔15〕事实上，即便是利益衡量，隐私敏感度在其中也扮演着至关重要的角色。〔16〕不过，大数据自动处理技术的出现，的确缩小了隐私信息和一般信息的鸿沟。分散的个人数据（如社保账号）如孤立地看，不太具有伤害性，可一旦与其他数据如金融信息结合，就变得异常敏感。因此，在原则上坚持领域理论的同时，也应注意使用场景对信息敏感度的影响，明确合理的隐私期待。

目前，民法之外的其他部门法对信息敏感度已有多处规定。如《征信业管理条例》第 14 条禁止收集医疗敏感信息，收集财产敏感信息则须有主体明示同意。“信息刑案解释”第 5 条对涉及四种不同敏感度信息的犯罪行为规定了轻重不同的刑罚。这些对于侵权法如何分类保护隐私信息和一般信息提供了重要参考。

对于隐私信息的侵害，原先可通过援引隐私侵权规则予以救济；对于非隐私信息的侵害，在民法总则实施前，司法实践往往通过其他路径来对个人信息予以保护。

“无讼阅读”数据库中“本院认为”部分含“个人信息”的民事判决书（截至 2017 年 9 月 30 日）

金融诈骗或盗窃纠纷(306)			征信错误纠纷	人格权纠纷(212)			医疗损害、委托合同等其他纠纷	判决总数
网银纠纷	伪卡交易	冒领信用卡、冒名贷款或冒领存款		名誉权	隐私权	其他人格权益		
152	77	77	73	101	75	36	11	602
25.25%	12.79%	12.79%	12.13%	16.78%	12.46%	5.98%	1.83%	100%

由上表可知，个人信息纠纷最常见的案型，是利用个人金融信息盗窃或利用个人信息进行金融诈骗，其次是人格权侵权，再次是征信错误纠纷。这些案件如今均可通过个人信息侵权制度予以解决。

（二）保护路径

关于侵权法保护个人信息的方式，比较法上有不同的路径。

美国有所谓信息隐私（information privacy）的概念，〔17〕将个人信息保护纳入到隐私保护之下。除了分散的法律法规（如美国宪法第四修正案等）与规章、指南（如美国联邦贸易委

〔11〕 BGH 36, 77, 80; BGH NJW 1987, 2667; NJW 1991, 1553; BVerfG 54, 148, 154; BVerfG NJW 1991, 2340.

〔12〕 前引〔7〕，王泽鉴书，第 200 页。

〔13〕 BVerfG 65, 1, 45.

〔14〕 前引〔4〕，杨芳文，第 113 页。

〔15〕 J. Hager, Staudinger, BGB-Neubearbeitung, Das Recht der unerlaubten Handlungen, 2014, Rn. 344.

〔16〕 除德国外，其他国家也有类似的领域理论，如从纯粹私域到纯粹公域的光谱理论。See B. J. Koops, B. C. Newell, *A Typology of Privacy*, 38 U. Pa. J. Int'l L. 544 (2017).

〔17〕 See Eugene Volokh, *Freedom of Speech and Information Privacy*, 52 Stan. L. Rev. 1049 (2000).

员会发布的《公平信息实践》（FIPs））外，隐私侵权法对个人信息提供了一般性的侵权保护。[18] 2018 年 6 月 28 日，美国加利福尼亚州议会通过消费者隐私法（California Consumer Privacy Act of 2018/Assembly Bill No. 375）。这部法律通过赋予信息主体广泛的知情权、访问权和删除权，强化个体对自身信息的控制。但该法仅为州法，并且迟至 2020 年 1 月 1 日才施行。

除欧盟《数据条例》外，德国法还提供了如下几种救济模式。其一，绝对权侵权救济模式。这种模式或是认为个人数据权（Recht am eignen Datum）本身就是德国民法典第 823 条第 1 款所称的“其他权利”，故可直接适用该款；[19] 或是认为个人信息自决权（informationelle Selbstbestimmung）虽不是该款所称的“其他权利”，但它属于一般人格权，[20] 而一般人格权是该款所称的“其他权利”，从而仍可适用该款。[21] 其二，违反保护性法律的侵权救济模式。德国刑法典第 303a 条（故意删改数据罪）以及德国数据法的大量核心条文（如第 28 条“为商业目的收集、存储他人信息”），被认为属于德国民法典第 823 条第 2 款意义上的“保护性法律”，从而受害人可以通过合并援引这些条文来获得侵权救济。[22] 其三，德国数据法第 83 条规定的损害赔偿请求权，该条包括 5 款，容后详述。此外，德国民法典第 824 条（危害信用）、第 826 条（故意背俗侵权）、第 831 条（事务辅助人责任）、第 839 条（公务人员责任），以及德国基本法第 34 条（国家赔偿责任），在不同场合下都有适用可能。[23]

除欧盟《数据条例》外，法国民法典主要提供两种救济模式，即人法之人格权保护模式和债法之一般侵权条款模式。法国民法典第 9 条第 1 款规定：“任何人均享有私生活受到尊重的权利。”侵害个人信息属于侵害他人私生活或宽泛的人格权，受害人可单独援引法国民法典第 9 条获得救济。而法国民法典第 1382 条系侵权责任一般条款，受害人在因信息侵害而遭受经济损失时常援引该条。这两个条文系补充关系，但因归责原则不同（第 9 条是无过错责任，第 1382 条是一般过错责任），法官援用后者呈减少趋势。[24]

以上三种模式中，美国模式对非隐私一般信息几乎不予保护，其对个人信息的保护明显不足。大多数美国隐私学者认为，“企业和政府对个人信息的收集与使用正处于失控状态（spinning out of control）”。[25] 法国民法典通过第一卷“人”第一编“民事权利”中的私生活（宽泛人格权）条款与侵权法一般条款，对个人信息提供双重保护，而德国民法典亦有多个侵权法条文可援用，另有其数据法上独立的索赔请求权基础。总体上，法、德两国民法对个人信息侵权提供了较为充分的救济。

在我国民法上，个人信息究竟是权利客体还是仅为一种利益载体，未有定论；但在个人信息遭受侵害时，民法（侵权法）同样提供了两种可能的救济路径：其一，侵权责任法第 36 条结合“信息侵权解释”的特别路径；其二，民法总则第 111 条结合侵权责任法第 6

〔18〕 See D. J. Solve & W. Hartzog, *The FTC and the New Common Law of Privacy*, 114 Colum. L. Rev. 583 (2014).

〔19〕 Münchener Kommentar zum BGB, 7. Auflage 2017, Wagner, § 823 Schadensersatzpflicht, Rn. 296.

〔20〕 Staudinger/Hager (2017), C. Das Persönlichkeitsrecht, Rn. C173, Rn. B140.

〔21〕 BGHZ 181, 328 Rn. 28 ff.

〔22〕 前引〔19〕，慕尼黑评注，第 823 条，边码 295。

〔23〕 BeckOK Datenschutzrecht, BDSG 2018, 24. Edition, 01. 08. 2017, Wolff/Brink, § 83, Rn. 9.

〔24〕 V. Hélène Pélissier-Gateau, JurisClasseur Civil Code > Art. 1382 à 1386, Fasc. 133 – 30: Droit a reparation, 25 Février 2015, no 245, 248.

〔25〕 Shawn A. Johnson, *A Law and Economics Approach to Privacy Policy Misstatements: Considering the Need for a Cost-Benefits Analysis in the FTC's Deception Framework*, 18 Colum. Sci. & Tech. L. Rev. 79, 81 (2016).

条的一般路径。前者为网络信息侵权责任的特别规定，仅适用于利用网络侵害他人信息的案型；后者为个人信息侵权的一般规定，适用于侵害他人信息的一切案型。以下就两种路径的构成要件予以分析。

二、新型损害的出现与部分认可

不论是何种路径的侵权法保护，损害均系传统事后救济型侵权责任的共同要件。在个人信息侵权场合，除信息主体隐私曝光而遭受精神痛苦这种典型损害之外，还出现了诸多新型损害，侵权法应有选择地予以承认。新型损害分述如下。

第一种，数据泄露。即个人数据被破坏、窃取或擅自访问，导致数据的保密性或完整性遭到破坏。如美国知名信用机构 Equifax 信息泄露事件、〔26〕美团个人数据泄露事件等。〔27〕数据泄露使得数据主体遭受后续次生损害的风险陡增。

第二种，导致或促成下游犯罪发生。即信息侵害作为下游犯罪的预备条件，下游犯罪包括但不限于网络攻击、诈骗、身份盗窃、敲诈勒索、跟踪杀人等等。例如，美国数据经纪商 Sequoia One 出售贷款申请人的金融信息，信息购买者遂冒名借贷或盗刷信用卡。〔28〕又如，Uber 公司搜集到某位记者的隐私信息，要挟警告其停止负面报道。〔29〕再如，新罕布什尔州一位居民购买某熟人的个人信息，后跟踪并将其杀害。〔30〕我国目前多发的各种精准诈骗亦属此类。

第三种，社会分选（social sorting）和歧视。所谓社会分选，是指收集个人数据，再依据多种标准（年龄、经济实力等）将人群分类，并决定谁应当有何种待遇。〔31〕“大数据黑名单”即基于分类筛选，推定部分人在社会管理领域“有罪直至其证明自身无辜”，从而限制其乘飞机、移民等等。〔32〕社会分选本身并无好坏之分，如“骑行狂热者”群组既可能对广告业主有用，也可被保险公司用于提高保险费率。〔33〕但更多时候，社会分选带来的是不当歧视。例如，低收入群组必须承受更高的贷款利率，冲动型人格群组的求职者可能被雇主排斥。顺风车用户被车主点评贴上各种标签，此类用户画像可被其他顺风车主在软件后台随意浏览，并作为接单时的筛选依据。〔34〕数据泄露或买卖使得分类筛选与歧视得以秘密

〔26〕 参见《Equifax 信息泄漏事件揭秘：美国信用体系存在致命缺陷》，http://tech.qq.com/a/20170909/025920.htm，2018 年 3 月 30 日访问。

〔27〕 参见《三重渠道泄露隐私数据，难道用户卸载美团才能自保?》，http://www.sohu.com/a/229216672_116553，2018 年 4 月 30 日访问。

〔28〕 CQ Roll Call Staff, *FTC Cites 2015 Successes in Privacy, Data Security Actions*, 2016 WL 2759289 (2016).

〔29〕 See Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U. C. Davis L. Rev. 1183 (2016).

〔30〕 See Remsburg v. Docusearch, Inc., 816 A. 2d 1001 (N. H. 2003).

〔31〕 David Lyon, *Surveillance as Social Sorting: Computer Codes and Mobile Bodies*, in David Lyon (ed.), *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination*, Routledge, 2002, p. 13.

〔32〕 Margaret Hu, *Big Data Blacklisting*, 67 Fla. L. Rev. 1735 (2015).

〔33〕 *FTC Recommends Congress Require the Data Broker Industry to be More Transparent and Give Consumers Greater Control Over Their Personal Information*, https://www.ftc.gov/news-events/press-releases/2014/05/ftc-recommends-congress-require-data-broker-industry-be-more.

〔34〕 《起底滴滴顺风车：上车前司机就知道你美不美了》，http://news.ifeng.com/a/20180511/58281058_0.shtml，2018 年 5 月 12 日访问。

化和便利化，受害人既无从知晓，也无法摆脱。

第四种，数据监控下的不安与自我审查。超强数据攫取能力令每个人形同透明，迫使个体谨言慎行，总是倾向于选择温和与主流。〔35〕互联网对个体思想数字表达的持续监控“令个体决策程序发生短路”。〔36〕个人自治空间和隐私空间被大幅压缩，私生活受到侵害。

第五种，消费操纵和关系控制。数据画像使得定向广告无比精准地在特定时间和场景到达目标用户，诱发冲动消费。商家“像对待石油那样对待消费者数据”。〔37〕这不啻是一种消费操纵。更恶劣的是关系控制（relational control），它是指利用秘密获取的他人信息对其在社会或职业网络中施加影响。〔38〕例如，招聘者在面试中发现应聘者在各方面都堪称知己，遂欣然同意雇用，但其实后者只是购买了前者的个人信息从而曲意逢迎。信息获取者在了解信息主体后通过伪装而影响后者决策，从而导致潜在的无法认知的损害。

上述五种新型损害对传统侵权法而言均较为陌生，很难获赔。首先，单纯的数据泄露，信息主体很难证明有实际损害。美国《计算机欺诈和滥用法》（CFAA）明确要求，信息被泄露的主体索赔时须证明存在“实质上的经济损害”。〔39〕在 Spokeo，Inc. v. Robins 一案中，被告擅自抓取原告个人数据并发布错误财产信息，美国最高法院判定，被告程序性违法本身并不足以自动满足“事实上侵害（injury-in-fact）”这项要件，即缺乏个别化和具体化的损害。〔40〕同样，在“李立彬与中国保险监督管理委员会隐私权纠纷”一案中，法院判定，原告未能证明因被告可能的数据泄露而遭受到实际损害。〔41〕

其次，在数据交易事实上已促成下游犯罪的场合，因果关系的认定是难题。在前述新罕布什尔州的信息主体遭跟踪杀害的案例中，美国法院迫于舆论压力而认定数据经纪人对其过失承担责任，但同时指出，此例外的责任承担与“普通市民没有保护他人免受第三方犯罪攻击的一般性义务”之原则相冲突。〔42〕在前述本文统计的 602 份判决中，因信息泄露导致金融诈骗或盗窃和人格权受侵害的案件中，原告的胜诉率分别为 51.63% 和 60.38%，即分别有五成和四成比例的受害人无法获得救济，主要原因是受害人无法证明被告的归因性和归责性。同样的困难也出现在利用大数据进行筛选和歧视的场合。

最后，监控导致的不安和自我审查以及消费操控、关系控制，传统观点倾向于否定其构成损害。在 Shibley v. Time，Inc. 案中，杂志出版商将用户的订购书目信息出售给邮件广告商，法院认为，尽管原告生活方式或会曝光，但书目信息的销售不会“引发常人的精神痛苦或屈辱感”。〔43〕同样，在 Dwyer v. American Express Co. 案中，法院认为，消费习惯数据画像的出售并不属于任何一种隐私侵权。〔44〕定向广告在我国同样很难构成损害。在“北京百

〔35〕 J. E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 Stan. L. Rev. 1426 (2000).

〔36〕 Paul M. Shwartz, *Privacy and Democracy in Cyberspace*, 52 Vand. L. Rev. 1656 (1999).

〔37〕 Andrew Hasty, Note, *Treating Consumer Data Like Oil*, 67 Fed. Comm. L. J. 293, 300 (2015).

〔38〕 See T. Rostow, *What Happens When an Acquaintance Buys Your Data?*, 34 Yale J. on Reg. 667 (2017).

〔39〕 See R. M. Peters, *The Problem with Current Data-Breach Notification Laws*, 56 Ariz. L. Rev. 1178 (2014).

〔40〕 Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1549 (2016). See S. E. Pugh, *Cloudy with a Chance of Abused Privacy Rights*, 66 Am. U. L. Rev. 1013 (2017).

〔41〕 参见北京市第二中级人民法院（2016）京 02 民终 3276 号民事判决书。

〔42〕 See Remsburg v. Docusearch, Inc., 816 A. 2d 1006 (2003).

〔43〕 Shibley v. Time, Inc., 341 N. E. 2d 337 (Ohio App. 1976).

〔44〕 Dwyer v. Am. Express Co., 652 N. E. 2d 1351 (Ill. App. 1995).

度网讯科技公司与朱烨隐私权纠纷案”中，原告朱烨诉称，百度未经其知情同意而收集其网页浏览记录（cookies），并对其实施精准营销从而使其紧张不安，侵害了其私生活安宁。法院认定隐私侵权不成立，重要理由之一是：原告没有证明个性化推荐服务“对其造成了事实上的实质性损害”。〔45〕

总体上看，大数据背景下的新型损害主要是数据泄露本身及其各种次生损害，这些损害难以被传统侵权法观念所接纳。其原因主要在于：其一，损害通常以侵害为前提，但在上述情形中，某些行为是否构成侵害、是否属于对信息的不法或不当处理，存在疑问，如网站以默示同意方式收集用户网页浏览记录并实施精准营销即为如此。其二，传统上，对于财产性损害的判定，通说采差额说，〔46〕而上述五种情形中，财产性损害往往尚未发生或尚未被发现，信息主体无法证明之。其三，对于非财产性损害，其赔偿须以法律特别规定为前提，〔47〕并需要达到“造成他人严重精神损害”（侵权责任法第 22 条）的程度，此项事实的证明对于信息主体而言亦绝非易事。

针对上述困境，有学者提出较为激进的主张，例如针对信息泄露和下游犯罪，“应扩大人身损害的范围，信息泄露导致被害人被抢劫强奸甚至杀害，泄露者应承担隐私侵权责任”；针对筛选和歧视，“应以侵犯隐私权来救济，而不仅仅是侵犯平等就业权”。〔48〕但事实上，这些主张存在若干认识误区，对上述新型损害应否由侵权法认可，不可一概而论。

首先，对于擅自传送的信息被用于下游犯罪，此处所涉问题其实不是“人身损害范围的扩大”，而是这种本应由犯罪人承担责任的人身损害在多大程度上可归咎于、归因于信息泄露者。一般情况下，后续损害不应由信息泄露者承担。只有当信息主体能够证明，信息泄露者明知或应知被泄露的信息将被用于后续加害时，之后的实际损害（遭受诈骗或盗窃等）才可归因于、归责于信息泄露者。〔49〕切不可在信息侵害与后续损害之间直接划等号。

其次，对于大数据导致的筛选和歧视，应分而论之。一是，对于敏感信息的获取、加工、转让以及使用，应取得信息主体的明示同意（《个人信息安全规范》第 5.5 条）。2018 年 1 月 4 日，支付宝就其暗中捆绑《芝麻服务协议》并代替用户默认勾选“同意”一事公开道歉，因该协议“服务规则”第 1 条规定：“您同意我们向第三方采集并在适用的法律法规许可的范围内向信息使用者依法提供这些信息……纳入这些消息对您的信用评级（评分）、信用报告等结果可能产生的不利影响……”。〔50〕该条实际上是支付宝谋求“合法取得用户数据并制作”数据画像，并将其向第三方“合法传输和提供”，所谓的“可能产生的不利影响”即各种社会分选或歧视。未经用户明示同意即收集和传输敏感信息，显然侵犯个人信息权益。同样，《个人信息安全规范》附录 B 明确例示：“在未取得个人信息主体授权

〔45〕 参见南京市中级人民法院（2014）宁民终字第 5028 号民事判决书。

〔46〕 参见曾世雄：《损害赔偿法原理》，中国政法大学出版社 2001 年版，第 129 页。

〔47〕 参见王泽鉴：《损害赔偿》，北京大学出版社 2017 年版，第 64 页。

〔48〕 徐明：《大数据时代的隐私危机及其侵权法应对》，《中国法学》2017 年第 1 期，第 146 页。

〔49〕 依“信息刑案解释”第 5 条，出售或提供的轨迹信息被用于犯罪的，不问出售者或提供者对此是否或应否知情，其一律构成侵犯公民个人信息罪。此时，在民法上，后续犯罪所致损害可否归因于信息出售者或提供者，值得探讨。

〔50〕 参见《支付宝深夜紧急回应年度账单质疑：我们错了，愚蠢至极》，http://tech.ifeng.com/a/20180104/44831532_0.shtml，2018 年 1 月 4 日访问。本文所引《芝麻服务协议》指的是 2018 年 1 月 3 日事发当日支付宝所使用的版本。

时，将健康信息用于保险公司营销和确定个体保费高低”，属于个人敏感信息的滥用。当然，只有在信息侵害者明知或应知该信息会被用于不当筛选和歧视时，被筛选和歧视这种新型损害才可归因于、归责于前者。

二是，在用户知情且同意的前提下，数据处理者制作数据画像并传输给第三方，后者利用该数据画像进行分组、筛选并用于企业决策，该行为或存在就业歧视等违法行为，但其本身并不构成个人信息侵权。不过，为防止用户数据画像被滥用，我国法可借鉴法国信息与自由法第10条、〔51〕欧盟《数据条例》第22条之规定，原则上禁止单纯依据数据画像等自动数据处理系统来对个人进行会产生法律后果的评价决策，而且任何情况下，自动数据处理系统的决策不得基于敏感类型数据（种族、基因数据、健康数据等）作出。

再次，关于数据监控、消费操控以及决策诱导，主要涉及上网痕迹（cookies）的收集、转让以及使用的合法性问题。关于收集的合法性，上网痕迹一般情况下可能并不敏感，但有例外，例如频繁搜索并登录治疗特定疾病的相关网站，此类上网痕迹有可能构成导致歧视性待遇的敏感信息。因此，对于用户上网痕迹的收集、处理、传播和使用，应采取区分立场。法国信息与自由委员会要求涉及社交媒体分享、受众评估研究（mesure d’audience）以及用于精准营销（publicité ciblée）等三类上网痕迹的收集，必须取得用户事先明确同意，以缓解上网痕迹滥用带来的“特别负面的效果”。〔52〕我国《个人信息安全规范》附录表B.1“个人敏感信息举例”第六类“其他信息”中，“网页浏览记录”（即cookies）也赫然在列。就此而言，前述百度未经用户明示同意即收集用户网页浏览记录，并用以作定向营销，也属于非法收集个人敏感信息。

关于使用的合法性，依广告法第43条，〔53〕擅自发送电子信息广告系违法行为，而频繁的广告轰炸则构成对隐私权（私生活安宁）的侵犯。德国法也是如此认定。“最近以来，越来越多的人将一般人格权用作抵抗不请自来的广告的法律手段。”〔54〕就此而言，擅自收集用户的上网痕迹而发布定向广告，既可能侵犯隐私权，也构成对个人信息的非法使用。至于利用合法收集的上网痕迹推送高度个人化定制的新闻，很难认定构成信息的非法使用。

关于转让的合法性，擅自收集用户上网痕迹并转售给广告公司用于精准广告投送，此行为本质上类似于“搜集个人资料寄发广告信函”，〔55〕我国台湾基隆地方法院依据旧个人资料保护法（1995）第28条判定后者构成侵害个人隐私，此判决值得参考。同时该行为也构成对个人信息的侵害（非法收集、非法出售）。

最后，关于数据泄露。若被泄露数据的主体无法证明存在实际经济损失，也无法证明存在严重精神损害，则按现行法似乎就不存在损害。然而，一方面，就经济损失而言，一向保守的德国法最近也开始承认若干新型数据损害，如“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”等等。〔56〕

〔51〕 法国信息与自由法（la loi Informatique et Libertés）制定于1978年，基于与欧盟《数据条例》保持协调一致，该法的最新版本于2018年6月20日颁布（La loi n° 2018－493 du 20 juin 2018）。

〔52〕 V. G. Desgens-Pasanau, La protection des donnees personnelles, 2e ed., LexisNexis, 2016, no. 320, p. 149.

〔53〕 该条规定，任何单位或个人未经当事人同意或者请求，不得以电子信息方式向其发送广告。

〔54〕 前引〔10〕，梅迪库斯书，第810页。

〔55〕 参见前引〔7〕，王泽鉴书，第244页。

〔56〕 前引〔23〕，Wolff/Brink评注，第83条，边码44。

我国“信息侵权解释”第 18 条也明文规定，“被侵权人因人身权益受侵害造成的财产损失无法确定的，法院可在 50 万元以下酌定赔偿数额。”据此，只要信息主体证明其信息权益这种人身权益遭受到了侵害，无须证明具体财产损失数额，法院也应酌定赔偿数额。

另一方面，就精神损害而言，旧德国数据法第 8 条第 2 款曾规定“严重侵害人格权”的要件，但新法第 83 条第 2 款已追随欧盟《数据条例》第 82 条，删除了这项要件，从而使得信息主体索赔精神损害的门槛显著降低。〔57〕“侵害人格权本身就足以构成损害。依审判实践，损害的概念应当宽泛地解释，并应适应欧盟关于自然人数据保护指令的目的和完整的保护范围。”〔58〕德国既往支持精神损害赔偿的判例包括：未经同意对信息主体进行 HIV 测试，在周报上将某女雇员标记为“最懒女同事”，以及雇主对雇员实施未经允许的视频监控等等。〔59〕值得一提的是，德国联邦宪法法院在 2010 年的一个判例中特别指出，“在数据泄露场合下创设通知义务、引入无过错责任或强化对非财产性损害的赔偿都可作为对技术性手段的补充，以强化实现有效数据保护的激励。”〔60〕另外，我国台湾个人资料保护法第 28 条第 3 款规定，“依前二项情形（即财产损害与非财产损害），如被害人不易或不能证明其实际损害额时，得请求法院依侵害情节，以每人每一事件新台币五百元以上二万元以下计算。”可见，该法对于侵犯个人信息的损害认定，不仅没有要求“严重侵害人格权”或者“严重精神损害”的要件，而且在受害人无法举证具体损害大小时，径自估定损害额。以此方式来认可和确定数据泄露的损害，不失为一种保护信息主体的适当办法。

总体而言，大数据背景下的个人信息侵权损害呈现出若干新特点：可发生于数据处理的多个环节，普通个体的信息亦具有经济价值从而导致信息侵害普遍化，以及信息损害具有衍生性和继发性等等。对于上述新型损害，一方面不可一概承认，导致信息处理者动辄得咎，而应在认定损害之前对处理行为是否构成侵害严格甄别，即对数据处理行为的合法性、合规性进行考察，并将数据处理利益与信息主体的信息利益进行衡量；另一方面，也不可拘泥于“严重精神损害”或“实际经济损失”而对其一概否认，在数据侵害场合下缓和此项要件已是一种趋势。

三、三元归责原则体系的确立

（一）直接侵权

侵权责任法第 36 条可适用于利用网络实施信息侵权的案型。一般认为，该条遵循的是一般过错责任原则，〔61〕与该法第 6 条第 1 款的归责原则相同。然而，在大数据背景下，对于信息侵权适用一般过错责任，对信息主体的保护不够。例如，数据泄露场合，信息主体很难证明存储者有过错，因为数据存储公司的过错（合理注意）标准极不清晰。〔62〕信息主

〔57〕 Bundesdatenschutzgesetz und Nebengesetze Kommentar, 5. Aufl. , Carl Heymanns Verlag 2017, Holger Greve, § 8, Rn. 34.

〔58〕 前引〔23〕，Wolff/Brink 评注，第 83 条，边码 44。

〔59〕 前引〔57〕评注，第 7 条（Philipp Kramer），边码 30。

〔60〕 BGH Urt. v. BGH 2. 3. 2010, BVERFG Aktenzeichen 1 BvR 586/08, Rn. 223.

〔61〕 参见张新宝、任鸿雁：《互联网上的侵权责任：〈侵权责任法〉第 36 条解读》，《中国人民大学学报》2010 年第 4 期，第 20 页。

〔62〕 Clara Kim, *Granting Standing in Data Breach Cases*, 2016 Colum. Bus. L. Rev. 544（2016）.

体甚至根本不知有侵权，也就更不可能证明有过错。在多个控制者多个处理环节中，要判断谁有过错就会越来越困难。

有鉴于此，旧德国数据法（2003）在信息侵权上采二元归责原则。该法第 8.1 条规定，公务机关违反本法或其他数据保护规定，“不被允许地或不正确地”运用数据自动化方式处理个人信息造成损害，应承担无过错责任。同时该法第 7.2 条对于公务机关采取非自动化方式处理数据，或者非公务机关处理数据，并导致信息主体损害的情形，规定了过错推定责任。最新德国数据法（2018）将这两个条文整合，规定在第 83 条第 1 款：若控制人处理他人数据的行为违反本法或其他可适用之法，并导致他人损害，则控制人或其权利行使者负有损害赔偿义务。在非自动化数据处理场合，若损害不可归因于控制人的过错，则赔偿义务取消。单纯从措辞上看，“无过错”“过错推定”等字眼消失不见，但事实上，无论是审判实践还是理论通说，仍坚持二元归责立场。〔63〕并且，因欧盟《数据条例》及相关指令“对于过错问题有意保持开放，将此问题交由各成员国立法者自行安排，故无过错危险责任与非自动处理场合下带有免责可能性的过错推定之规定，是与欧洲法相一致的立法安排”。〔64〕

值得一提的是德国法上的不法性要件。新德国数据法直接使用“违反本法或其他可适用之法”，而旧德国数据法所称的“不被允许或不正确地”处理数据，也“应被理解为‘不法地’，它是指数据处理的任一环节未获信息主体同意，或者欠缺数据法或其他法律规定的法定授权依据，或者违反其他义务性规定（如通知义务）”。〔65〕应注意的是，不法性要件的证明责任不在信息主体一方；“按照表见证明之原则，信息主体只需证明公务机关处理了其数据”。〔66〕这种证明责任分配模式与欧盟《数据条例》第 5 条第 2 款的规定是一致的。

另外，当信息主体主张德国民法典第 823 条第 2 款的请求权时，适用过错推定责任。根据审判实践，“当保护性法律被违反时，（作为剩余部分）的过错，亦即内在注意的违反也将会被认定”。〔67〕当然，受害人必须证明行为人“客观上违反保护性法规”，但“保护性法规自身包含了特殊的证明分配规则的除外”。〔68〕这意味着，德国数据法或欧盟《数据条例》关于数据处理合法性的证明责任由数据处理者负担这项规则，在此场合仍可适用。

在我国台湾，某银行因过失致受害人征信错误并影响其申请贷款，法院以旧个人资料保护法为“保护性法律”判定银行担责，其“主要实益在于推定行为人的过失”。〔69〕而新个人资料保护法第 28 条、第 29 条规定，公务机关和其他主体违反本法规定造成信息主体损害的，分别负担无过错责任和过错推定责任。但是，相对于公权力行使的标准而言，是否采用数据自动处理（大数据）技术，〔70〕才是归责原则问题上更具有决定性意义的标准。

本文认为，个人信息侵权应采三元归责体系。首先，公务机关以数据自动处理技术实

〔63〕 前引〔23〕，Wolff/Brink 评注，第 83 条，边码 48，51。

〔64〕 同上引评注，第 83 条，边码 19。

〔65〕 前引〔57〕评注，第 8 条（Holger Greve），边码 15，18。

〔66〕 同上引评注，第 8 条（Holger Greve），边码 24。

〔67〕［德］埃尔温·多伊奇、汉斯—于尔根·阿伦斯：《德国侵权法》，叶名怡等译，中国人民大学出版社 2016 年版，第 108 页。

〔68〕 前引〔19〕，慕尼黑评注，第 823 条，边码 543。

〔69〕 前引〔7〕，王泽鉴书，第 171 页。

〔70〕 自动化数据处理是指对技术系统和人工系统尤其是信息技术（IT）的采用。参见前引〔23〕，Wolff/Brink 评注，第 83 条，边码 49。

施的信息侵权，应适用无过错责任。因为政府是最大的数据控制者和管理者，而大数据实际上强化了政府和个体既有的力量强弱差序格局。〔71〕个体无论从财力上、技术上还是从举证和诉讼能力上，都越来越无法与公权力机构抗衡。自动化数据处理技术会给人格权带来一种典型的“自动化危险”，而在人工处理数据的场合，这样的风险并不存在。“通常的过错责任要求受害人承担无限制的证明义务，而自动化数据处理具有特殊性，如技术上无限的可能性，错误数据也能永久存储，能够无远弗届、即刻检索、调阅数据，此二者不相适应。考虑到对局外人而言几乎不可能追根溯源的复杂工序，在自动化处理场合下，不能苛求信息主体必须证明设备的运营者有过错，因而德国数据法规定了此种无过错的危险责任。”〔72〕我国网络安全法第 74 条规定：“违反本法规定，给他人造成损害的，依法承担民事责任。”该条规定的显然也是无过错责任。但是，一方面，它不区分是否为公务机关，也不区分是否采用了大数据技术，一律设定为无过错责任，此种立法模式难称精细；另一方面，该法对于损害赔偿责任新增了“违法性”要件，但又未明确哪一方对此承担证明责任。在解释论上，依我国行政诉讼法第 34 条，当数据处理者为行政机关时，数据处理行为的合法性应由行政机关证明；当数据处理者为其他主体，同时又未采用大数据技术时，违法性证明宜由数据主体承担，以缓和无比宽泛的无过错责任可能带来的负面影响。

其次，采用自动化处理系统的非公务机关，其信息侵权应适用过错推定责任。相对于采用大数据技术的公务机关而言，同样采用了大数据技术的非公务机关，由于缺少了公权力行使的便利，其掌握的资源相对较少，其获取数据、分析处理数据的能力相对较低，故对其课予的注意义务标准也应相对调低。同时，考虑到大数据技术本身的复杂性，在此场合下，对其设定过错推定责任较为妥当。在比较法上，数据处理者的过错推定责任适用范围很广。除上文讨论过的德国数据法、我国台湾个人资料保护法的相关规定外，欧盟《数据条例》第 5 条第 2 款规定，数据控制者对其符合第 1 款之数据处理各项要求（合法性、合理性、透明性、目的限定、数据最小化、准确性、完整性和机密性）承担证明责任。从条文表述看，当涉及对他人信息的处理时，不仅有不法性推定，还有不合理性、不当性等其他推定。故有学者认为，它隐含了过错推定原则，数据控制者要证明损害不应归责于自身。〔73〕欧盟法的这项规定不区分处理者是否公务机关，是否采用数据自动化，一律采过错推定，其侵权责任成立的门槛更低。考虑到当事人双方地位变化系因大数据而产生，同时也为了与传统隐私侵权一般过错之归责保持一致，宜将过错推定责任限定为运用数据自动化技术的场合。另外，针对网络安全法第 74 条规定的“基于违法性的无过错责任”，从解释论出发，当信息处理者为非公务机关时，数据处理行为的违法性应由信息主体承担证明责任。但从立法论出发，应废止如此宽泛的无过错责任，转采有梯度的三元归责，针对采用了数据自动处理技术的非公务机关设定过错推定责任，同时将合法性的证明责任课予数据处理者。事实上，鉴于大数据技术的隐蔽性和复杂性，令信息主体证明数据处理行为有违法性，其难度不亚于要求其证明信息处理者有过错。

---

〔71〕 See Amy J. Schmitz, *Secret Consumer Scores and Segmentations*, 2014 Mich. St. L. Rev. 1411.

〔72〕 前引〔57〕评注，第 8 条（Holger Greve），边码 5，9。

〔73〕 V. C. Terwangne1, K. Rosier et B. Losdyck, Lignes de force du nouveau Règlement relatif à la protection des données à caractère personnel Revue du Droit des Technologies de L'information-N° 62/2016, no 42, p. 28.

最后，未采用自动数据处理系统的数据处理者，其信息侵权应适用一般过错原则。因为争讼双方举证和诉讼能力上的差异主要是大数据处理技术带来的，而不论数据控制者是否为网络服务提供商。不过，鉴于实践中大数据运用的广泛性以及普通个体举证能力的欠缺，应推定数据控制人采用了自动数据处理系统。〔74〕未利用网络（通常也不会采用大数据技术）而侵害他人个人信息的案件，适用前述侵权保护的一般路径，即侵权责任法第6条第1款配合民法总则第111条。根据前者规定，信息主体应证明信息处理者存在过错，但不必证明信息处理行为的违法性。

（二）间接侵权

数据处理者除承担直接侵权责任外，还可能作为网络服务商承担间接侵权责任，因为数据处理的外延很宽泛，既包括数据收集，也包括存储、共享等等。当个人信息被第三人发布于网络平台时，网络平台作为信息存储者可能承担间接侵权责任。

在比较法上，此种责任大致有三种立法例：（1）美国媒介中立理论。美国《通讯端正法》（Communication Decency Act）第230条c（1）规定："任何互动式计算机服务的提供者或使用者都不应被视为其他的信息内容提供者所提供信息的发布者或言说者。"与《数字千年版权法》（Digital Millennium Copyright Act）针对版权侵权所确立的"通知—撤回"避风港规则不同，《通讯端正法》第230条c（1）针对网络用户的言论侵权，为网络平台提供了极其广泛的免责。〔75〕网络服务提供商即使收到名誉或隐私被侵犯的用户投诉却仍不清理有害信息，或被证明存在过失，也能免责。〔76〕（2）欧洲避风港（safe haven）原则。依欧共体电子商务指令（2000/31/EC）第14条，从事数据存储的媒介不承担责任，除非其明知存在非法内容或在接获用户投诉后仍不删除。英国诽谤法（Defamation Act）第5条规定，网络运营者原则上不对用户言论承担责任，除非受害人投诉却不予回应，或受害人无法识别和起诉信息发布者。（3）加拿大分发者（distributor）理论。网络服务商被视为信息的分发者，承担过错推定责任，其应证明对有害言论不知情且无过失。〔77〕

媒介中立理论的前提其实并不存在，它完全无视网络平台对其所承载信息的控制力。避风港模式兼顾各方利益，适用范围最广，也为侵权责任法第36条第2、3款所采纳。通说认为其归责原则是一般过错责任。〔78〕国外有学者认为，这种通知后必须撤除否则承担责任的模式，近似于一种严格责任。〔79〕我国另有学者主张，对网络内容服务提供商（ICP）和平台服务提供商（IPP）适用过错推定原则。〔80〕

本文认为，侵权责任法第36条第2款所确立的避风港原则，首先是一个责任豁免条款。对于网络平台来说，即使在其网站上存储有侵害他人权利（该第2款未区分人格权和著作权）的有害信息，只要在接获受害人通知后及时删除，即可免责。其次，倘若依据该条第2

〔74〕 德国法也作此种推定。参见前引〔57〕评注，第8条（Holger Greve），边码9。

〔75〕 Matthew Schruers, *The History and Economics of ISPs for Third-Party Content*, 88 Va. L. Rev. 205 (2002).

〔76〕 Michal Lavi, *Content Providers' Secondary Liability: A Social Network Perspective*, 26 Fordham Intell. Prop. Media & Ent. L. J. 855, 869 (2016).

〔77〕 See A. Bernstein & R. Ramchandani, *A Discussion of ISP Liability*, 1 Can. J. L. & Tec. 79, no. 2 (2002).

〔78〕 参见程啸：《侵权责任法》，法律出版社2015年版，第448页。

〔79〕 M. Thompson, *The Normative Responsibility of Internet Intermediaries*, 18 Vand. J. Ent. Tech. L. 848 (2016).

〔80〕 前引〔48〕，徐明文，第146页。

款，网络平台最终被认定负有侵权责任，则该责任的归责原则应为过错推定责任。从文义解释出发，只要用户有投诉，网站就必须撤除争议信息，否则一旦信息最终被认定为错误或违法，网站即须承担责任。这种“通知—撤除”模式将“知悉信息存在”与“知悉信息违法”等同起来，完全不考虑不同网站的审查能力，也不考虑它在评判争议内容违法性时是否尽到合理注意义务。请求权人只须证明信息有害、已进行通知、网站未及时删除即为已足，他无须证明网站违法或网站能注意而未注意，即无须证明其有过错。

四、复数控制人场合下的因果关系推定

因果关系是所有类型侵权责任的共同要件。因果关系要件可分解成两个问题：其一，谁是行为人；其二，行为人的特定行为（或状态）是否构成特定损害（或侵害）的原因。就此而言，个人信息侵权救济的最大难题其实是因果关系的证明。因为数据收集、处理、转移以及使用等多个环节中，每个环节都可能发生数据不当泄露，信息主体很可能无法确定行为人的范围，即使确定范围后也无法证明其中哪一个是真正的行为人，即使证实是特定行为人后也无法证明后者的何种行为正是数据侵害结果发生的原因。〔81〕

例如，在“去哪儿机票信息泄露案”中，庞某委托鲁某通过“去哪儿”网订购东航机票，联系人信息为鲁某及其手机号，但庞某手机却于两日后收到诈骗短信。一审法院以庞某无法证明二被告存在过错为由驳回其诉请。二审法院认为，二被告存在泄漏原告个人隐私信息的高度可能，判决侵权成立。〔82〕显然，法院是基于生活经验和概率论，运用司法推定（并非法律推定）解决了信息传递多重环节中因果关系的证明难题，以避免原告举证不能而无法获得保护的不公平结果。有学者主张，在信息侵权中，为减轻信息主体的证明负担，因果关系判断宜采“条件说”，涉及本案任何一个环节的主体均可作为侵权主体而被追诉。〔83〕这是对条件说的误解和误用。因为条件说即“but for”标准恰恰无法解决多因一果问题，这才有聚合因果关系、共同因果关系或择一因果关系等多数因果关系理论的出现。而且条件说过于宽泛，若不配合相当因果关系理论，侵权责任赔偿范围将缺乏有效的限制性工具。

针对复数数据控制人场合下的因果关系证明难题，域外法多采因果关系推定。例如，欧盟《数据条例》第 82.3 条规定，复数控制者和/或处理者牵涉同一侵害性数据处理时，若控制者或处理者能够证明其无论如何都不应对致害事件负责，则可以免责。最新德国数据法第 83 条第 3 款（旧法第 8.4 条）也明确规定：在自动化数据处理场合，如果不能查明多个数据控制人中的哪一个引发了损害，则每个控制人或其权利实施者都承担责任。“这种复数行为人之连带责任的前提要件是：存在两个以上的数据控制人，且不能查明致害原因；于此场合存在因果关系的缓和，即请求权人不必证明，损害可相当性地归因于数据处理行为。由此，发动者身份（Urheberschaft）的证明与致害原因力份额的证明，都得以缓和。”〔84〕

〔81〕 Ignacio N. Cofone, *The Dynamic Effect of Information Privacy Law*, 18 Minn. J. L. Sci. & Tech. 552 (2017).

〔82〕 参见庞某与北京趣拿信息技术有限公司等隐私权纠纷案，北京市第一中级人民法院（2017）京 01 民终 509 号民事判决书。

〔83〕 前引〔48〕，徐明文，第 146 页。

〔84〕 前引〔23〕，Wolff/Brink 评注，第 83 条，边码 30。

为何要在自动化数据处理的复数控制人场合实行因果关系推定？因为德国立法者认为本条规定与德国民法典第830条第1款第2句（共同危险行为）本质相同，“（复数控制人）这种共同起作用的关系使得因果关系的证明复杂化。因为请求权人没有任何洞察力，以弄清联合性的数据处理的内部过程……他也没有能力查明各控制人之间的任务分配和协作关系。”〔85〕即使在非自动数据处理的场合，虽不能适用本条规定，但德国民法典的一般性规则仍然适用，因此，民法典第830条第1款第2句（共同危险行为）也会导致同样的因果关系推定。〔86〕其实，在旧数据法时期，德国理论甚至认为，在单个数据控制人的场合，“数据主体也只须证明其有损害，而无须具体证明损害与责任机关的数据处理之间的因果关系”，“数据控制人可以通过证明其数据处理行为与损害之间没有因果关系来免责”。〔87〕

显而易见，在单个控制人的场合也进行因果关系推定，此立场过于激进，不宜借鉴。至于欧盟《数据条例》不区分是否使用大数据技术，只要是复数控制人场合就一律实行因果关系推定，也过于激进。因为信息主体之所以难以证明因果关系，主要原因有两点：其一，复数行为人（至少客观上）的行为协同；其二，大数据技术的高度复杂性。本文认为，只有在复数控制人采用大数据技术的场合，才应确立因果关系推定规则。这种场合下，受害人无论从技术上还是财力上，都无法准确查证到底是哪一个或哪几个数据处理者实施了侵害行为，这种困难是一种客观的现实存在，立法若不解决则受害人在此场合下根本不可能获得有效救济。上述“去哪儿”网案中仅有两名被告，基于生活经验的司法推定尚可奏效，若多达十几个数据处理人时，司法推定将不敷使用。在因果关系推定规则建立之前，可参考德国法经验，类推适用侵权责任法第10条（共同危险行为）的规定。

五、自成体系的预防性责任措施

当个人信息遭受侵害但尚未出现损害时，信息主体可诉诸侵权责任法第21条规定的预防性侵权责任。这种前瞻性的侵权责任在责任构成、法律效果上均与向后看的传统损害赔偿侵权责任有重大差别。在构成要件方面，它不要求有损害和过错，只要求有不法侵害或迫近的危险。关于个人信息的预防性责任措施，也指向停止侵害和消除危险，具体包括更正、停止处理、断链、删除、隐名化等数字加密处理等。

信息更正权是指信息主体有权要求信息控制者及时更正其不正确、不准确或不完整的信息。欧盟《数据条例》第16条与我国网络安全法第43条对此均有规定。随着数据画像愈发普遍，更正权也愈发重要。因为数据画像会分析不同场景下多个分离的数据，却没有额外信息解释它们之间的关系，很容易导致数据画像扭曲和失实。〔88〕美国最大的数据经纪商承认，高达30%的数据画像可能是错误的。〔89〕而在我国，据本文统计，迄今信息主体以征信错误为由要求更正的案件数占总数（602例）的比例为12.13%，比例不低。

〔85〕 同上引评注，第83条，边码33。

〔86〕 同上引评注，第83条，边码34。

〔87〕 前引〔57〕评注，第8条（Holger Greve），边码24；第7条（Philipp Kramer），边码20，22。

〔88〕 See D. J. Solove, *Public Records, Privacy and the Constitution*, 86 Minn. L. Rev. 1185 (2002).

〔89〕 M. Hicken, *Find out What Big Data Knows about You*, http://money. cnn. com/2013/09/05/pf/acxiom - consumer - data/.

停止处理权，是指当数据错误或保护不足，或数据处理系非法但不宜删除时，信息主体有权要求信息控制人暂时或永久停止数据处理。这在欧盟《数据条例》第 18.1 条、第 21.1 条以及德国数据法第 36 条、第 58 条均有规定。但我国网络安全法仅规定了更正、删除以及采取确保信息安全的措施，未规定这种停止处理权，应予完善。

删除权，是指当数据处理系非法或原初目的已实现或无法实现时，数据主体有权要求数据控制者及时删除其个人信息。与其相近的被遗忘权，是指数据主体对于网络上误导性的、令人难堪的、不相关的或过时的个人数据，有权要求数据控制者予以断链或删除。〔90〕欧盟法院曾在“西班牙谷歌案”中对其作了确认。〔91〕不过，由于被遗忘权会导致“强制沉默”和言论审查，〔92〕加之欧盟自身对全球性断链权（de-listing）缺乏合意，〔93〕因此，欧盟《数据条例》第 17 条最终使用的标题是“删除权（被遗忘权）”，明显采折中妥协模式。〔94〕

在我国，基础意义上的删除权在侵权责任法第 36 条、网络安全法第 43 条均有体现，但被遗忘权目前法无明文规定。有的学者主张建立完整意义上的被遗忘权，即允许将“不恰当的、过时的、会导致信息主体社会评价降低的信息”删除。〔95〕“被遗忘权将人们从对过去的恐惧中解放出来，反而会强化言论自由。”〔96〕但也有学者认为，应建立范围有限的删除权制度，因为被遗忘权乃至删除权不仅在技术上不具有可操作性，〔97〕还可能使我国企业失去国际市场竞争力。〔98〕

本文认为，第一，不能因特定网络信息无法彻底删除就否认删除权的重大意义。事实上，对于防止信息扩散而言，删除网络链接比删除原作内容页面要有效率得多。第二，被遗忘权使得网络企业（搜索引擎）被迫对他人言论予以审查，有压制言论自由的风险，且执行成本过高，不利于我国互联网企业发展。第三，现有删除权制度适用范围过于狭窄，应予扩充。一方面，应扩大义务主体范围，从“网络服务提供者或运营者”扩至一切数据控制者或处理者；另一方面，应扩张适用场合，可删除者不仅包括“实施侵权行为的信息”、“违法或违约收集、使用的信息”，还应包括对于原初目的而言已不必要的信息、撤回同意或原来法定依据现已丧失的信息。第四，在权利行使效果上，信息主体通过撤回同意而行使删除权时，数据控制者应从服务器上删除包括元数据在内的一切个人数据。但在有偿许可他人收集信息场合下，删除权人应对相关损失承担赔偿责任。

在个人信息出于科学研究等公益目的而被收集或使用时，或面临数据泄露或被滥用危险时，信息主体还可以要求信息控制人增强保卫措施以消除危险。其中，隐名化技术处理是重要措施之一，它也是在尊重人格和表达自由（信息不被删除）之间保持平衡的重要手段。

---

〔90〕 M. J. Kelly, D. Satola, *The Right to Be Forgotten*, 1 Ill. L. Rev. 3 (2017).

〔91〕 See Case C-131/12, Google Spain SL v. Agencia Espanola de Proteccion de Datos, 2014 E. C. R. 317.

〔92〕 V. A. Bretonneau, Le droit au «déréférencement» et la directive sur la protection des données personnelles, RFDA 2017, p. 535.

〔93〕 V. O. Tambou, les difficultés de la mise en oeuvre du droit européen au déréférencement, RTD Eur. 2016, p. 249.

〔94〕 I. G. Bădescu, Le droit à l'oubli numérique: De l'Europe au Japon, Revue de l'Union européenne, 2017, p. 153.

〔95〕 杨立新、韩煦：《被遗忘权的中国本土化及法律适用》，《法律适用》2015 年第 2 期，第 32 页。

〔96〕 郑志峰：《网络社会的被遗忘权研究》，《法商研究》2015 年第 6 期，第 58 页。

〔97〕 鞠晔、凌学东：《大数据背景下网络消费者个人信息侵权问题及法律救济》，《河北法学》2016 年第 11 期，第 56 页。

〔98〕 万方：《终将被遗忘的权利——我国引入被遗忘权的思考》，《法学评论》2016 年第 6 期，第 162 页。

隐名化分为假名化与匿名化。假名化（pseudonymisation），是指对个人数据的加密处理，如用标签取代姓名和其他识别性标记等，使得若不使用另外单独存储的额外信息就无法或难以再识别数据主体（欧盟《数据条例》第4.5条、德国数据法第22条第2款与第46条）。匿名化（anonymisation）是指对个人数据进行修改，使得无法再根据相关信息识别特定的自然人，或只有花费不成比例的时间、金钱和劳动的情况才能进行识别。假名与匿名存在重要区别。将文件名移除后用数字替代，并分别储存在不同文件中，这本身并没有使数据匿名化，而只是假名化。即使不显示名字，个人数据也可以通过适当工作付出而连接到特定主体，假名化的数据仍然受欧盟《数据条例》的调整。而真正匿名化的数据，必然已经过实质性修改，因此难以再将其回溯至被识别或可识别的自然人。〔99〕

尽管从技术角度说，匿名化的保护力度远强于假名化，但它仍不足以完全消除数据泄露或滥用的危险。虽然商业企业经常以隐名化或匿名化来回应消费者的隐私关切，然而，目前已知大量的去匿名化技术，可以轻松地帮助人类和计算机重新识别匿名化的数据。此类技术主要包括外部连接攻击、采集者关联攻击以及数据属性关联攻击等。〔100〕外部连接攻击是指攻击者利用辅助信息或背景知识去识别匹配的数据库，此方法特别有效。〔101〕例如，S. J. Lewis揭示，一个包含1.7亿行程、匿名驾照、牌照和其他元数据的20GB匿名数据库，可轻易地通过匹配信息被破解，包括准确识别驾驶员身份。〔102〕

反向识别技术对于中国这样一个网络实名制泛化的国家尤其具有威胁性。因为几乎所有的（半）官方数据库（如电信、交通、银行、快递、支付系统等），都使用同一套基础性身份验证系统（姓名+身份证+手机号），而且线上线下没有隔离。这意味着用来比对匹配的辅助数据库异常丰富，反向识别难度大幅降低，故立法应对匿名数据库的储存和管理予以规定。尽管如此，相对于显名数据，个人数据的假名化和匿名化处理仍有必要，特别是匿名化对于数据识别设置了成本和技术上的高门槛，对于防范信息主体遭受潜在威胁具有重要意义。

六、责任形态的更新及其多样化

信息侵害行为造成信息主体损害，应承担损害赔偿责任。其中非金钱赔偿方式包括恢复原状、消除影响、恢复名誉、赔礼道歉。“信息侵权解释”第16条规定，赔礼道歉、消除影响或者恢复名誉等责任形式，应当与侵权的具体方式和所造成的影响范围相当。另外，更正、断链、限制处理、删除、隐名化等手段，在损害发生后，也可作为恢复原状的具体措施。

“信息侵权解释”第17条、第18条对金钱赔偿的数额进行了规定：（1）能确定实际损失的按实际损失，包括针对数据分析行为的调查和防御费用，如符合国家有关部门规定的律师费等。（2）损失难以确定的按侵权人的获利数额。（3）侵权人获利也难以确定的，由法院在50万元以下酌定。另外，对于非财产性损害，如隐私披露，信息主体可以主张精神损害赔偿，此点为侵权责任法第22条、《关于确定民事侵权精神损害赔偿责任若干问题

〔99〕 See Article 29 Working Party, Opinion 05/2014 on Anonymisation Techniques, https://perma.cc/HZT6-B7EV.

〔100〕 金欣煜：《数据采集与分享中隐私保护方法研究》，上海财经大学管理科学与工程专业2017年博士论文，第102页以下。

〔101〕 Xuan Ding *et al.*, *A Brief Survey on De-anonymization Attacks in Online Social Networks*, 2010 Int'l Conf. on Computational Aspects of Soc. Networks 611, 614.

〔102〕 Sarah Jamie Lewis, *Please Stop Releasing "Anonymized" Datasets*, LinkedIn Pulse, Jan. 25, 2016.

的解释》（法释〔2001〕7 号）第 1 条所确认。对于牟利性恶意侵犯个人信息，从有效遏制和预防角度出发，应借鉴德国人格权保护中对惩戒功能的重视，[103] 引入惩罚性赔偿。[104]

更复杂的是复数侵权人的责任形态问题。本文认为，大体有三种可能：连带责任、补充责任和按份责任。第一种连带责任，首先可能源自狭义的共同侵权。当复数数据处理者构成所谓的联合控制者（joint controllers）时，数据主体可以针对每个数据控制者行使权利（欧盟《数据条例》第 26 条）。当复数数据处理者造成同一损害时，每一个控制者或处理者都应当对整个损害承担连带责任，以确保对数据主体的有效赔偿（欧盟《数据条例》第 82.4 条）。这种连带责任本质上是因为共同侵权而引发的。我国侵权责任法第 36 条第 3 款规定的正是网络服务提供者与信息发布者共同侵权的连带责任，而第 2 款实质上也是推定接获通知仍不采取措施的网络服务者具有过错（故意），同样是共同侵权下的连带责任。

其次，连带责任还可能源自广义的共同侵权。又可分为两种，即帮助侵权和共同过失侵权。明知他人利用个人信息实施犯罪或侵权，仍向其出售或提供个人信息的，依据侵权责任法第 9 条，非法出售者或提供者应与直接侵权人承担连带责任。传统见解认为，共同侵权范畴下的帮助行为仅限于故意，否则帮助人虽构成侵权，但不承担连带责任。[105] 不过，我国台湾 2010 年“台上字第 1058 号判决”判定，过失帮助行为亦导致连带责任。[106] 而我国最高人民法院认为，传统上无过错能力的“无民事行为能力人”也可以实施帮助行为，此情形“可认定为共同侵权行为”。[107] 这种帮助行为概念的扩大化，是对传统“故意帮助行为”概念的突破，其目的在于扩大连带责任的适用范围。不过，倘若承认复数行为人的共同过失也能成立共同侵权，[108] 则是否扩张“帮助行为”并不那么重要。知道或者应当知道他人利用公民个人信息实施信息侵权，仍向其出售或者提供的，显然与直接侵害人有共同的过错（故意或过失），二者应承担连带责任。

再次，连带责任还可能源自共同危险行为。如前所述，在采用数据自动处理技术的复数控制人的场合，德国法类比共同危险行为，实行因果关系推定。我国现行法对此无专门规定，但侵权责任法第 10 条规定了共同危险行为，于此场合，可类推适用之。

第二种是未尽到安保义务的补充责任。民法总则第 111 条明文规定，“任何组织和个人需要获取他人个人信息的，应当依法取得并确保信息安全。”据此，数据控制人对用户个人数据负有安全保障义务，若其因未尽安保义务（过失）导致个人数据被第三人窃取或破坏，或是遭泄露的数据被第三人用来从事犯罪或侵权，并给信息主体带来损害，这种情形下，一方面，作为直接加害人的第三人固然要承担侵权责任，但另一方面，数据控制人也应在其过错范围内承担相应的补充责任。因为补充责任适用的典型场合之一正是“第三人介入时违反安全保障义务的侵权责任”。[109] 在数据泄露的场合，直接侵害人与安全保障义务人也

〔103〕“在衡量赔偿数额时应强调对媒体企业的预防功能，以防止无所顾忌的不法人格权廉价出售得不到惩戒。”参见前引〔67〕，多伊奇等书，第 241 页。

〔104〕前引〔48〕，徐明文，第 149 页。

〔105〕前引〔78〕，程啸书，第 375 页。

〔106〕王泽鉴：《侵权行为》，北京大学出版社 2016 年版，第 443 页。

〔107〕最高人民法院侵权责任法研究小组编：《〈中华人民共和国侵权责任法〉条文理解与适用》，人民法院出版社 2010 年版，第 83 页。

〔108〕前引〔106〕，王泽鉴书，第 436 页；前引〔107〕，最高人民法院侵权责任法研究小组编书，第 69 页。

〔109〕张新宝：《我国侵权责任法中的补充责任》，《法学杂志》2010 年第 6 期，第 2 页。

处于“不同的责任层次或级别”,[110] 完全符合补充责任的本质。当然，这种虚拟场所（电子数据储存网站）下的安保义务及其补充责任宜由立法直接明文规定。

第三种是分别侵权场合下的按份责任。例如，非法出售或提供非敏感的个人信息，该信息被他人用于针对信息主体的侵害行为（如歧视），但出售者或提供者对此不知情且无重大过错。这种情况下，出售信息和歧视这两种过错相互结合后造成同一损害，各行为人应根据侵权责任法第 12 条承担按份责任。

七、结论及展望

大数据在深刻改变人类生活的同时，也给个人信息安全带来前所未有的威胁。如何为个人信息提供侵权法保护，是当今值得严肃对待的一项重要课题。本文研究结论如下：

一切具有可识别性的个人信息均受侵权法保护，侵权法对非敏感个人信息提供保护不会阻碍信息流通。敏感信息和非敏感信息的侵权法保护力度存在差异，二者的鸿沟虽因数据画像而缩小，但并未消灭。个人信息侵权构成应予适当缓和。应承认若干新型损害，如数据泄露、擅自收集上网痕迹用于定向广告导致的人格权损害等等。应建立三元归责体系，即针对使用自动数据处理系统的公务机关、非公务机关以及未使用该系统的传统信息侵害行为分别适用无过错、过错推定以及一般过错责任。在复数数据控制人采用大数据技术的场合应建立因果关系推定规则。侵害个人信息但尚未造成损害时，可适用预防性侵权责任，具体措施包括更正、停止处理、删除以及隐名化等措施。应在过失帮助侵权、共同过失侵权以及不确定因果关系等场合下新增连带责任。同时，将安保义务及其被违反导致的补充责任扩张，以适用于作为虚拟场所管理人的数据存储者。

因此，大数据技术给人类带来了巨大的潜在风险，引发了新的损害，加剧了个体与信息处理者之间的强弱对比，从整体上颠覆了传统侵权法框架所赖以建立的基础场景。为因应新形势，必须在信息侵权领域重构侵权法框架。有一种论调认为，个人信息弱保护模式有利于企业做大做强，因而我国应学美国而非欧盟。但事实上，从 2000 年欧美之间的《安全港协议》，再到 2016 年 7 月 12 日《隐私盾协议》（Privacy Shield），最后到 2018 年 5 月 25 日起生效的欧盟《数据条例》，美国在近二三十年数据立法方面一直处于价值被输出国地位；而欧洲《数据条例》“正在塑造新的全球标准”,[111] 成为欧盟对世界发挥影响力的重要支撑。[112] 事实上，美国法也在转向。例如，2018 年加州消费者隐私法为消费者创设了四项强有力的权利：知情权、访问权与可携带权、删除权、拒绝信息被出售权,[113] 这些权利几

---

〔110〕 参见李中原：《论违反安全保障义务的补充责任制度》,《中外法学》2014 年第 3 期，第 693 页。

〔111〕 B. A. Safari, *Intangible Privacy Rights: How Europe's GDPR Will Set a New Global Standard for Personal Data Protection*, 47 Seton Hall L. Rev. 847 (2017).

〔112〕 Maïka Bernaerts, Les transferts de données à caractère personnel entre l'Union européenne et les Etats-Unis: une valse à mille temps1?, R. D. C. 2017/2, p. 184.

〔113〕 该法案第 1798.100 条（a）（b）（c）规定，消费者有权知晓其何种信息被收集、收集目的；同时，（d）规定了消费者享有访问权和可携带权。第 1798.105 条规定了消费者的删除权，“消费者有权要求企业删除从前者处收集的任何相关个人信息”，此项删除权甚至比欧盟《数据条例》的删除权还要宽泛和强有力。第 1798.120 条规定了消费者的拒绝信息被出售权，“消费者有权在任何时候指令向第三方出售消费者信息的企业，不得出售消费者的个人信息”。第 1798.125 条规定，企业不得对行使本法规定之信息权利的消费者实施任何歧视。

乎是欧盟《数据条例》中数据主体权利的翻版。又如，2018 年 6 月 22 日，美国最高法院裁决，警方只有在获取法庭批准的搜查令后，才能获取嫌疑人手机上的过往轨迹信息；而在此之前，警方可直接从无线运营商那里获取此类数据，此举被认为违反美国宪法第四修正案。〔114〕

更重要的是，个人信息弱保护模式在伦理和效率上都是有疑问的。在中国这样一个在线上线下各领域全方位落实实名制的国家，与美国背景完全不同，采用弱保护模式将会给个人隐私带来深重灾难；同时，法经济分析表明，一定程度的隐私保护可以促进更多的信息公开和更多的信息产生。〔115〕当前，我国对个人信息的侵权法保护不是过强而是过于宽松，信息产业野蛮生长，信息买卖畸形繁荣，各种信息滥用如精准电信诈骗屡屡发生。值此之际，应强化公、私法协同，除了应尽快出台《个人信息保护法》之外，编纂中的民法典之侵权责任编还应发挥后发优势，建构明晰的个人信息侵权规则，这对于保护民众权益、更新民法理论以及推进社会发展均具有重大意义。

Abstract: All kinds of personal information are protected by tort law, and tort law protection of non-sensitive personal information does not hinder the flow of information. Tort law provides two protection paths for personal information. One is the network information infringement clause of Article 36 of the Tort Liability Law and its judicial interpretations, and the other is the fault infringement clause of Article 6 of the Tort Liability Law in conjunction with Article 111 of the General Principles of Civil Law. The constituent elements of personal information infringement should be appropriately moderated by recognizing a number of new types of damages, constructing a system of ternary imputation principles, and establishing a causal relationship presumption in the case of plural controllers. In the area of personal information infringement relief, importance should be attached to the use of preventive liability methods, such as correction, stop processing, deletion, and digital encryption. With regard to monetary compensation, joint liability provisions should be added to the Law in the case of (negligent) contributory infringement, uncertain causality, etc., and the security obligation and its supplementary liability caused by the violation should be expanded to apply to the manager in virtual place (data storage). In the context of the pan-real name authentication system, China should choose an information protection model that is closer to the European, rather than the American model.

Key Words: personal information, tort law, constitutive requirements, preventive liability, forms of liability

〔114〕 Carpenter v. United States, No. 16 - 402. Argued November 29, 2017—Decided June 22, 2018, https://www.supremecourt.gov/opinions/17pdf/16 - 402_new_o75q.pdf.

〔115〕 前引〔81〕，Cofone 文，第 571 页。