大数据时代的隐私危机及其侵权法应对

徐　明*

内容提要　Web2.0标志着大数据时代的到来，也意味着隐私危机的到来：隐私侵权变得十分容易、普遍，行为方式变得更加隐秘，性质更难以确定，后果多样化且程度更严重，行为与结果之间的因果关系更松散。我国传统的间接保护隐私权的方式已远远落后于时代。为扩大隐私侵权救济之可能性，有必要重新构筑侵权规则：明确以隐私权保护而非个人数据保护为基点的路线；采取形式的隐私权定义加实质判断标准相结合的方法判定隐私利益的存在；扩张隐私损害结果的范围；适用过错推定原则以增加被侵权人胜诉之可能性。

关键词　大数据　隐私权　侵权法　责任扩张　过错推定

引　言

Web2.0的出现标志着大数据时代的开启，人类收集、存储、分析数据的能力达到了前所未有的高度。大数据正越来越深刻地改变着现存世界，甚至“改变了人类对知识的定义”[①]，已经引起了各学科的精英们强烈的关注。大数据通常在以下三个语境中被提及：一是指超强的收集、存储、及时、精确地处理数据的能力；二是指借助各种类型工具对数据进行比较、分析；三是指一种方法论意义上的观念，即大数据有助于更客观、精确地发掘真相与事物之间的关联性[②]，其核心在于预测[③]。不可否认，大数据的这些特性的确可以帮助人类解决长期困扰人类的难题：环境保护、国家安全、犯罪防控、健康预

* 武汉大学法学院博士后研究人员，武汉工商学院教授。本文系湖北省医事卫生法律治理研究中心资助的博士项目（项目批准号：D2014007）的阶段性成果。

① Danah boyd and Kate Crawford, Six Provocations for Big Data. A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society, September 2011.

② *See* Danah Boyd & Kate Crawford, Critical Questions for Big Data: Provocations for a Cultural, Technological, and Scholarly Phenomenon, 15 INFORMATION, COMMUNICATION, & SOCIETY p. 662-679 (2012).

③ Charles Duhigg, How Companies Learn Your Secrets, N. Y. Times, Feb. 19, 2012, http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html.

防、市场预测、恐怖袭击的预测与防范等④,但同时也带来了隐私危机⑤。

大数据使得隐私侵权变得十分容易、普遍,侵权行为方式变得更加隐秘,侵权性质更难以确定,侵权后果多样化且程度更严重,侵权行为与结果之间的因果关系更松散。凡此种种,无不对侵权规则的适用构成了严重的挑战,导致法律救济的困难。有人悲观地预言,"大数据时代,隐私权已死"⑥,也有人极端地认为应废除隐私权的概念,"透明社会对社会各阶层都有益"⑦。但这些论调完全否定了隐私权对于人类社会的积极意义,并不可取。有论者提出了系数隐名技术⑧和基于上下文隐名技术⑨。但技术更新速率过快使得刚刚适用的技术便已经失去了作用。还有人提出了财富分享的理论⑩,试图以适当的经济补偿来消除隐私危机。然而财富分享则面临无法确定分享的范围和程度的问题。显然,这些方法都不能从根本上解决大数据时代隐私危机带来的挑战。

笔者认为,大数据时代隐私权危机的主要症结在于当前法律框架下的责任范围不足以完成保护隐私权的使命,虽然"以往的法律框架已经不再适用"⑪,但并未崩溃,可以做出适当的调整以扩展责任范围,提高救济的可能性。况且,侵权法作为一种平衡各种利益的制度设置,更具灵活性,可以发挥更多的作用。基于这种考虑,笔者拟从完善隐私侵权法的角度来探讨应对大数据时代隐私侵权的危机。

一、网络隐私侵权:防不胜防

大数据最核心的技术特征就是超强的收集、存储、及时、精确地处理数据的能力以及精准的预测能力,这些特征对隐私存在天然的侵袭性。除此之外,信息的价值逐渐显露,无论是对个人、商家还是政府来说,信息都是一个丰富的宝藏,催生了一大批与信息利用相关的产业,也改变了人们的生活方式。个人不再仅仅作为信息源而存在,而更多地成为了自愿通过服务平台发布海量信息的积极参与者。如此一来,私人领域与公共领域的界限开始模糊,个人信息可以在所谓陌生的朋友之间广为流传。信息的收集者

---

④ Omer Tene &Julos Polonetsky, Privacy in the age of Big data: A Time for Big Decisions, 64. STAN L. REV. ONLINE 63 (2012).

⑤ Daniel J Solove, 'A Taxonomy of Privacy (2006) 154 Penn. Law Review 477, 506. Dirk Helbing and Stefano Balietti, Big Data, Privacy, and Trusted Web: What to Be Done, From social data mining to forecasting socio-economic crises. EPJ Special Topics 195, 3-68 (2011)

⑥ http://www. euronews. com/2014/01/06/big data big brother and the death of privacy in the digital age/

⑦ David Brin, The Transparent Society Will Technology Force US to Choose Between Privacr And Freedom? 245(1998)

⑧ L. Sweeney. k-anonymity: a model for protecting privacy. International Journal on Uncertainty, Fuzziness and Knowledge-based Systems, 10 (5),2002; 557-570.

⑨ Helen Nissenbaum, Privacy in Context: Technology, Policy, And The Integrity of Social Life (Stanford Law Books 2009).

⑩ Omer Tene and Jules Polonetsky, 'Big Data for All: Privacy and User Control in the Age of Analytics,' (forthcoming) Northwestern Journal of Technology and Intellectual Property.

⑪ Ira Rubinstein, Big Data: The End of Privacy or a New Beginning, NYU School of Law, Public Law Research Paper No. 12-56.

和利用者不再由政府或者少数机构垄断，个人、组织或者企业等也参与进来，这使得控制和监管变得十分困难，再加上元数据的模糊性，导致了种种隐私危机的出现。

其一，大数据时代超强的数据收集能力增加了隐私侵犯的可能性。博客（BLOG）、简易信息聚合 RSS、百科全书（Wiki）、网摘、社会网络（SNS）、对等网络（P2P）、即时信息（IM）等典型的 Web2.0 技术，使得人类活动的任何痕迹都可能作为数据被储存起来。再者，大数据时代自媒体风靡全国，不加区分地随意公布自己的信息及随意转载他人信息，往往也容易造成隐私侵权纠纷。凡此种种，使得收集他人信息、刺探他人的隐私变得十分容易，滥用信息的情况屡见不鲜，有人甚至倒卖收集到的信息。然而，网络营运商将敏感信息泄露给身份盗窃的黑客，或者将处理过的信息泄露给广告公司却很难得到司法救济。

其二，数据分析、挖掘是一种在大数据库中发现或推断未知事实的模式，它不依赖于因果关系而依赖相关性进行预测和推断，新发现的信息是非直观的，不具可预知性，整个过程相当不透明。[12] 很多公司都在从事这种业务，预测性广告就是其中一种，可以根据已知的信息推断出被侵权人不欲为他人所知的敏感信息，以至于被侵权人自己都没有意识到的隐私都有可能被他人知晓，比如，国外最著名的案例是刊载在纽约时报上的“推测少女怀孕并披露给商家”一案[13]。我国也有类似的案例出现。预测性广告还可能导致价格歧视和不平等。不仅如此，大数据时代的信息挖掘技术也使得以前的非敏感数据变成敏感性数据，比如，Stan Karas 教授论证了消费者信息较之以前具有更多的敏感性，属于隐私权保护的范畴。[14] 预测性广告可能导致更为严重的隐私侵权，但侵权法却很难对之加以规制。这是因为：数据的收集与分析都是以消费者看不见的方式进行的，即使消费者怀疑被伤害，可能也不知道谁起诉，或者缺乏必要的证据证明侵权者的责任和要求赔偿，[15]消费者看到广告时也可能没有意识到这是预测性广告，更不知道自己的哪个消费行为和哪些内容被收集和分析了。[16] 此外，由于预测性广告分析者根本不需要知道每个客户的身份信息，因而很难证明不当披露之诉中的因果关系——客户无权要求分析者提供任何与其名字相关的所有信息。

其三，反向身份识别技术使得网民几乎成为透明人。法律要求数据的收集者隐去

---

[12] U M Fayyad et al., 'From Data Mining to Knowledge Discovery, An Overview,' in U M Fayyad et al. (eds), Advances in Knowledge Discovery and Data Mining 6 (Menlo Park: AAAI, 1996), cited in Tal Z Zarsky, 'Mine Your Own Business! Making the Case for the Implications of the Data Mining of Personal Information in the Forum of Public Opinion' (2003) 5 Yale Journal of Law and Technology 1.

[13] Charles Duhigg, How Companies Learn Your Secrets, N. Y. Times, Feb. 19, 2012, http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html.

[14] Stan Karas, Privacy, Identity, Databases, American University Law Review. Volume52. Issue 2. p. 393-443(2002).

[15] *See* In re DoubleClick, 154 F. Supp. 2d at 526 (dismissing the plaintiffs' claims in part because their Computer Fraud and Abuse Act claim did not support a sufficient claim for damages).

[16] Fed. Trade Comm'N, FTC Staff Report: Self-Regulatory Principles For Online Behavioral Advertising I-II (2009) [hereinafter Principles]. p. 33-37.

资料提供者的姓名等信息，比如医学研究中收集的患者资料，遵循惯例都略去了患者的姓名、年龄和性别，但反向身份识别技术使这种惯例失去了意义。有关研究表明，仅需根据邮政编码、生日和性别，87%的美国公民可以被准确地识别身份。[17] 根据网上搜索痕迹也很容易确定搜索者身份。纽约时报曾报道过这样一个案例[18]：塞尔玛·阿诺德，一个62岁的寡妇，生活在格鲁吉亚的利尔本，在互联网上搜索了"60岁的单身男性"、"狗小便"和"手指麻木"就被人据此锁定了身份，从此永无宁日。

其四，大数据时代增进人体感官的技术层出不穷。感官增强技术使人们能够从"墙外"获得以往必须通过物理性侵入私人住宅才能获得的信息，其效果等同于对住宅实施了物理性侵入的效果，这种行为的法律属性是否也等同于非法搜查呢？比如，在Kyllo v. United States[19]一案中，美国内政部的一名探员怀疑Kyllo种植大麻从而使用热成像仪扫描器住宅以探测住宅内释放的热量是否适宜室内种植大麻。该案后来引起了广泛的争论。谷歌街景以其强大的功能受到全球网民追捧，但也饱受质疑：有人能通过谷歌街景地图意外发现已经离世祖母的身影；有女子遭男友赶出门的尴尬经历被谷歌拍到，上传到网络；还有人在自家前院小便被抓拍，要求谷歌赔偿一万欧元。[20]

其五，大数据时代隐私侵权的后果发生了变异。网络空间的可搜索性和永久存续性使得人们冀望于随时间而淡忘的期待落空，导致精神损害、名誉损害的长期化，从而加重损害的结果。比如，少女被性侵的视频或图像可能被长期地保存在网络上，这会给受害人造成难以承受的精神压力。[21] 身份盗窃也可能导致个人的信誉下降而丢失工作。更有甚者，罪犯可能利用网络上的不当披露的信息进行犯罪活动，包括信用卡盗窃、强奸、杀人等。[22] 我国也出现过利用大学生信息进行诈骗导致他人死亡的案例。

简而言之，大数据时代的隐私对侵权法的挑战主要集中在以上几个方面：第一，侵权主体难以确定，信息收集主体多元化，元数据利用方式多样化，以及侵权方式的隐秘性使得主体难以被发现；第二，信息的价值性使得侵权法的设置要兼顾多方面的利益，难以平衡；第三，隐私与个人信息直接的关系更加难以捉摸，有些信息在一定的条件下可以转化成隐私利益，给立法造成困难；第四，损害结果呈现多样化的趋势，不再局限于

---

⑰ Latanya Sweeney, Simple Demographics Often Identify People Uniquely 16 (Laboratory for Int'l Data Privacy, Working Paper No. 3, 2000); cf. Daniel C. Barth-Jones, The "Re-Identification" of Governor William Weld's Medical Information: A Critical ReExamination of Health Data Identification Risks and Privacy Protections, Then and Now 2 - 3 (July 24, 2012) (pre-publication working paper), available at http://dx. doi. org/10. 2139/ ssrn. 2076397; see also Latanya Sweeney, Akua Abu & Julia Winn, Identifying Participantsin the Personal Genome Project by Name 2 (Harvard Coll., Data Privacy Lab, White Paper No. 1021-1, Apr. 24, 2013).

⑱ Michael Barbaro & Tom Zeller Jr., A Face is Exposed for AOL Searcher No. 4417749, N. Y. TIMES, Aug. 9, 2006, at A2, available at http://www. nytimes. com/2006/08/09/technology/09aol. html.

⑲ Kyllo v. United States, 533 U. S. 27 (2001).

⑳ http://www. godeyes. cn/html/2008/04/07/google_earth_1610. html.

㉑ *See* John Schwartz, Child Pornography, and an Issue of Restitution, N. Y. Times, Feb. 3, 2010, http://www. nytimes. com/2010/02/03/us/03offender. html.

㉒ Daniel J. Solove, The Future of Reputation: Gossip, Rumor And Privacy on The Intenert, p. 100(2007).

名誉受损等精神损害,经济利益、不公平对待、人身损害等也时有发生发生,且精神损害的强度极大增强;第五,损害结果与行为直接的因果关系往往无法查明。凡此种种,导致被侵权人难以获得救济。

二、传统保护:捉襟见肘

相较于欧美近百年的隐私保护的历史,我国并无保护隐私权的传统,甚至也没有隐私的概念,与之相近的概念为阴私,意指男女之间的事,其外延远较现代隐私的概念要窄。更为重要的是,阴私只是一个伦理道德意义上的概念,没有发展演化为法律意义上的概念,更不用说发展成现代隐私权。这与家族主义和集体主义的文化传统不无关系,在这种文化氛围中,隐私权形成最重要的基石——个人自由——是不被重视的。据学者考证,1987 年以前,大陆未曾发表过有关研究隐私权的文章,1988 年以前,大陆的立法或司法解释中也未曾使用过"隐私"这一概念。[23] 改革开放以后,随着社会的发展与权利意识的觉醒,隐私权逐渐被重视,但总体上来说,我国公民保护隐私权的意识不强,大数据时代隐私保护又面临诸多窘境。

1986 年《民法通则》仅规定了姓名权、名誉权、肖像权等作为人格权间接地保护隐私权。1990 年《最高人民法院关于 < 中华人民共和国民法通则 > 若干问题的意见》虽然提出了隐私的概念,但仍将其作为名誉权的一部分间接地加以保护。1993 年《最高人民法院关于审理名誉权若干问题的解答》也是将隐私权纳入名誉权的范围来进行保护的。2001 年《最高人民法院关于确定民事侵权精神损害赔偿责任若干问题的解释》将隐私权作为一项独立的人格利益来进行保护,但受害人仅能请求精神损害赔偿。

但是,名誉权、肖像权、姓名权只占大数据时代隐私侵权的极小部分,保护的范围过于狭小,远远不能满足大数据时代隐私权保护的需要。不仅如此,间接保护路径的条件过于苛刻:侵犯肖像权的成立须"以营利为目的",而在大数据时代,即使不以盈利为目的,滥用他人肖像的行为也会导致极大的危害,但却很难以侵犯肖像权而得到救济;侵犯名誉权的成立须"以侮辱、诽谤等方式"进行,而"侮辱、诽谤"并无明确的标准,完全依赖于法官的自由裁量,何况即使制定像刑法上的侮辱、诽谤罪那样明确的标准,也不符合侵犯名誉权的实质,因为使他人社会评价降低并不需要达到"侮辱、诽谤"的标准。至于以精神损害来保护隐私权,也回避了问题的实质:一方面,侵害隐私权若以造成的原告之精神紧张的症状如失眠、记忆力减退等为依据,也只是以主观叙述为依据,舍此没人能证明自己失眠、记忆力减退等;若以造成的精神疾病为依据,则与个体差异有关,对彼人毫无作用的精神压力可能导致此人的精神崩溃,也容易导致审判结果不公,造成同样的行为导致不同的结果,因为就精神损害提起诉讼,"一般只有造成严重后果的才

---

[23] 参见张新宝:《隐私权的法律保护》,群众出版社 1997 年版,第 12 页脚注。

能得到实质救济";[24]另一方面,如前所示,侵犯隐私权所导致的损害远不止精神损害。

2008 年审结的号称"人肉搜索第一案"的"王菲诉张乐弈及网站"案可以更为直观地说明间接途径的缺陷。第一,本案是通过保护名誉权来保护隐私权的,但其所叙述的被侵权人出轨的事实都是真实的,若无捏造"逼死贤妻"之事实,被侵权人的人格评价降低是侵犯隐私权的结果吗?人格评价降低往往很难量化判断,多依赖于侵权人侵权行为的严重程度,这意味着间接途径依赖于损害结果的做法并非有效率的最佳选择。第二,网站在起诉前删除涉案帖子,能否据此判断不构成侵权?按照当前的侵权法的原理,网站是否侵权应看损害结果是否发生,现代网络的复制性使得有些行为一旦实施损害的结果就意味着损害的结果必定会发生,虽然存在一定的时间差。对于一些极具威胁性的隐私侵权行为,是否可以将处罚的阶段提前呢?另外,起诉前删除帖子只是减轻损害的措施,只能减轻责任而已,不是消除责任。第三,大数据时代侵权方式发生了巨大的变化,共同侵权十分普遍,参与人肉搜索的网友,是否应承担共同侵权的责任以及如何承担共同的侵权责任呢?

事实上,在本案判决的前后,我国陆续还出现不少利用信息网络侵害人身权益的典型案例,多以个案判例的形式形成了不同的规则,但没有普遍的效力,难以在全国范围内推广。比较普遍被认可的有以下规则:精神损害赔偿应与侵权人的过错程度相适应;[25]不宜仅以侵权信息的出现即认定网络服务提供者知道侵权事实的存在;[26]公众人物发表网络言论时应承担更大的注意义务;[27]被侵权人的影响力是判断经济损失的重要因素;[28]"影射"者的责任:从信息接受者的视角判断;[29]原告有权通过诉讼方式要求网络服务提供者提供侵权人的相关个人信息。[30] 这些案例所确立的原则或规则一方面表明了我国在网络侵犯隐私权方面法律规定的不足,同时也反映了我国法院系统对此作出了巨大的努力,为将来应对网络隐私侵权指引了方向,为后来的立法提供了论据。

然而,尽管在我国名人状告网络隐私侵权成功的比率已达 60% 左右,[31]但根据我国现有的法律规定,要想胜诉还面临三个方面的困难:一是难以证明被告存在侵权行为,隐私权常常与新闻媒体的言论自由、舆论监督权和社会大众的知情权等相冲突,且很难与学术评论等界分,缺乏相应的规则;二是难以证明损害结果,比如,社会评价降低的结果就只是一种笼统的观念反映,其范围和程度很难进行量化分析,导致事实认定困难;三是难以证明索赔金额的合理性,经济损失的数额难以量化,标准存在差异,很难得到

㉔ 参见《最高人民法院关于精神损害赔偿的司法解释》第 1 条、第 8 条。

㉕ 参见《徐大雯与宋祖德、刘信达侵害名誉权民事纠纷案》,北大法宝。

㉖ 参见《蔡继明与百度公司侵害》,北大法宝。

㉗ 参见《北京金山安全软件有限公司与周鸿祎侵犯名誉权纠纷案》,北大法宝。

㉘ 参见《赵雅芝与上海琪姿贸易有限公司、上海诺宝丝化妆品有限公司侵害姓名权纠纷、肖像权纠纷案》,北大法宝。

㉙ 参见《范冰冰与毕成功、贵州易赛德文化传媒有限公司侵犯名誉权纠纷案》,北大法宝。

㉚ 参见《闫某与北京新浪互联信息服务有限公司、北京百度网讯科技有限公司侵犯名誉权、隐私权纠纷案》,北大法宝。

㉛ 中外名人名誉侵权案层出不穷 媒体败诉率占 60%, 载 http://news.tuxi.com.cn/news/1199999990123403/34037271.html. 最后访问时间:2016 年 8 月 17 日。

法院认定,若以患有精神疾病的诊断证明作为索要较大数额的精神损害赔偿的依据,则证明精神病与侵权行为的因果关系更是十分困难。

由此可见,传统间接保护隐私权的路径不仅范围十分狭窄,而且效果有限。

三、个人信息保护:可预见的失败

经过一段时期的个案探索之后,2010年7月开始实施的《侵权责任法》确立了隐私权作为一项独立的人格权的地位,与肖像权、名誉权、姓名权等并列。但笔者认为,这与《民法通则》相比,除了以法律的形式明示了隐私权之外,并无太大的进步。

随着网络利用个人信息侵权的案例剧增,全国人大常委会于2012年12月28日通过了《关于加强网络信息保护的决定》(以下简称《决定》),但立法者很快便注意到该《决定》可诉性方面存在的缺陷:"能够识别公民个人身份和涉及公民个人隐私的电子信息"过于抽象,无法界定个人信息保护的范围;《决定》虽然规定了用户实名上网的义务,但仍存在部分用户没有实名登记,即使对于实名登记的用户,被侵权人也难以掌握涉嫌侵权的网络用户的身份信息,导致诉讼成立要素欠缺;网络提供者总以"不知道"侵权内容为由,要求适用"避风港原则",拒绝承担责任。

鉴于此,2014年6月,最高人民法院通过了《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》(以下简称《规定》),注重解决被侵权人诉讼难的问题:首先,明确了个人信息保护的范围及其例外原则;其次,划定了网络服务提供者"知道"的标准;再次,明确了网络用户或者网络服务提供者转载网络信息行为的过错及其程度的判断标准。

从立法思路来看,我国试图以个人信息保护来解决大数据时代的有关隐私的侵权问题的,为此立法上新创设立了不少义务,可以作为诉讼依据。但也存在自相矛盾的地方,反映了我国立法者对于个人信息和隐私的关系所持的态度十分暧昧。《决定》第1条将"能够识别公民个人身份"的电子信息和"涉及公民个人隐私"的电子信息并列十分令人费解,"涉及公民个人隐私"的电子信息无疑是针对某特定个人的隐私,应属于"能够识别公民个人身份"的电子信息,而现代隐私权认为"能够识别公民个人身份"的电子信息在特定的情形下属于隐私保护的范围,立法者到底是觉得前者过于宽泛而采用后者加以限制还是笼统地保护前者呢?不得而知。更为吊诡的是,《规定》第12条干脆将"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"直接等同于个人隐私,但保护的范围不仅仅限于这些个人隐私,还包括"其他个人信息",当然,从语法上来讲,"其他个人信息"应可以与上述等同于隐私的信息相当,这似乎表明立法者还是试图借助于隐私权来限定个人信息保护的范围。总之,我国立法者在路径的选择上摇摆不定,但总体上是倾向于效仿欧美,以数据保护法来代替隐私权保护的。

以欧盟和美国为例,二者皆很早就有《个人信息保护法》类似立法,且近期都根据大

数据的特点进行了修改或另行立法，但都因存在不可克服的困难而归于失败。从《欧洲数据保护法》实施来看，情况并不理想。2010 年 11 月，欧盟委员会发布了题为《欧洲范围内全方位的个人数据保护方法》的通讯文章，[32]指出技术的飞速发展和全球化给个人信息保护带来了极大挑战，尽管欧盟指令的原则仍然有效，但仍要强化数据保护，欧盟委员会发起了一场声势浩大的多方利益相关者协商，最后提交了 2012 年 1 月的立法方案，旨在改革欧盟指令。草案修改的内容十分广泛，其中有些修改得到了商界的赞许，但更多的部分却被认为不具有可操作性，是灾难性的。比如：增加了限制数据分析的条款、遗忘权、数据的可携权、一站式服务、影响评估以及数据保护委员会等。但上述改革仍没触及欧洲数据保护法的核心原则，包括数据质量（目的限制、数据最小化、精确、完整）、同意、透明、可接近与修改、保密与安全等。然而，这些原则“在大数据时代仍需在各个方面予以加强”[33]；“数据保护法太依赖于知情选择，经验表明，很少有人认真地阅读隐私条款，何况隐私条款用语模糊且变化莫测”[34]。

类似地，美国在 2010 年左右也进行了类似的改革。美国商务部和联邦贸易委员会于 2010 年检视了信息隐私框架，并出版了信息隐私和互联网创新调查报告，[35]2012 年 2 月出版了白宫最终报告：《网络环境下消费者数据的隐私保护——在全球数字经济背景下保护隐私和促进创新的框架》。[36] 该法案确立了一系列消费者权利，这些权利使消费者能够对企业如何处理其个人信息有明确的预期，同时也规定了消费者的义务；此外对信息的公平利用原则进行了重述，具体包括：透明、情景一致、安全、接入权与准确性、收集控制和问责制等。但其实质仍是注意——选择模式，不少论者认为作用不大。[37]

以此为鉴，我国以个人信息保护代替隐私权的保护并非明智之举。理由如下：

第一，个人信息与多种权利相关，比如，隐私权、姓名权、肖像权、名誉权、知识产权、商业秘密等都可以表现为个人信息，但也正因为其与多种权利相关，保护起来更为困难，因为很难以一种同质的权利对其本质进行概括而构筑大体相近的侵权规则。

第二，在限制范围方面，个人信息保护并不比隐私权来得容易。郭瑜认为个人信息

---

[32] A Comprehensive Approach on Personal Data Protection in the European Union, COM (2010) 609 final (Nov. 4, 2010) [hereinafter A Comprehensive Approach], available at http://ec. europa. eu/health/data_collection/docs/com_2010_0609_en. pdf.

[33] Omer Tene & JuloPolonetsky, Big Data for All: Privacy and User Control in the Age of Analytics, 11 Northwestern Journal of Technology and Intellectual Property 239 (2013).

[34] Fred H Cate, 'The Failure of Fair Information Practice Principles,' in Jane K Winn (ed.), Consumer Protection in the Age of the Information Economy 360 (Burlington: Ashgate, 2006).

[35] Notice of Inquiry, 75 Fed. Reg. 21226-31 (Apr. 23, 2010).

[36] The White House, Consumer Data Privacy in a Networked World: A Framework For Protecting Privacy And Promoting Innovation in The Global Digital Economy 32 n. 39 (Feb. 2012) [hereinafter The White House Blurptiny], available at http://www. whitehouse. gov/sites/default/files/privacy-final. pdf. An annex to the Report includes a table comparing the Consumer Privacy Bill of Rights to the OECD Guidelines and other documents. Id. At7.

[37] 4 Ira S. Rubinstein & Nathaniel Good, Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents, 28 BERKELEY TECH. L. J. (forthcoming 2013), available at http://lsr. nellco. org/nyu_plltwp/347.

属于一种新型的“个人数据权”[38]。笔者并不反对构筑一种新型的权利，但是，倘若这种权利缺乏有效的救济手段，或者尚需借助于其他权利进行保护，最佳选择肯定不是另起炉灶，还不如先完善被借助的那种权利侵权规则，因此，从现实的角度来看，现阶段立法者不应该试图以个人信息保护来代替隐私权的保护，而恰恰相反，应先完善隐私权的侵权规则。事实上，郭瑜列举的所谓“即使在最宽泛的‘隐私保护’的观念下，也很难照顾到”[39]的情形中，有一部分属于伪命题，比如“将个人信息发布到网上可以被浏览但不可被下载或保留”，因为“不能被下载”可以通过技术手段实现而不需要法律手段实现，且即使被下载或保留，若不加以利用、不产生危害，又怎么可能侵权呢？其余的部分情形，如银行、政府部门、邮政部门收集并生成新数据，利用或者不利用的情形等，正是数据挖掘的内容，而数据挖掘可能侵犯隐私权已经为大多数学者所承认，比如，Stan Karas 教授论证了消费者信息属于隐私权保护的范畴。[40] 可见，隐私权还有相当的扩展空间，试图以个人信息保护代替隐私权保护并非明智选择。

第三，个人数据所有权人具有可变性。依法收集和利用的数据，独立的个体所占的比例微乎其微，所有权当属数据收集者，但若该数据被滥用而导致侵权纠纷，该由谁来负责进行诉讼则不无疑问。

第四，个人数据的法律属性并不固定，有些数据在特定上下文中属于敏感信息，在一般情况下则不是，这给侵权规则的构建造成极大困难。与之相反，以隐私权为基准则有利于侵权规则的构建，因为这一系列与信息有关的侵权行为毕竟有一定的同质性。

第五，数据保护离不开知情选择模式，但在大数据时代，该模式事实上被虚置了。Web2.0 使个人数据更容易被收集、存储和侵犯，用户在网上的任何痕迹，不管是否告知，网络服务商都已经采集了所有有关用户的数据，不仅如此，当前网络服务商处于强势地位而网络用户处于弱势地位的情况下，即使网络服务商以隐私保护合约来履行告知义务，“告知与许可”原则也只是一个摆设，因为用户的同意带有明显的被强制色彩，用户不同意就无法享受服务。

第六，诸如数据最小化、匿名化等原则，在大数据强有力的反向识别和预测性挖掘等技术下，早已失去了应有的价值，不能起到保护隐私权的作用。

从理论上看，个人信息保护很难成功。从实践来看，我国立法中还有很多困难，比如，《规定》并没有很好地解决以下问题：同意例外是否需要充分知情？知情同意与公共利益的冲突如何解决？公共利益的必要性范围的界限是什么？不足以识别特定自然人的标准是以行为时还是法律制定时的标准为准？网络服务提供者是否“知情”的客观因素及网络用户或者网络服务提供者转载网络信息行为的过错及其程度的判断标准是由法院依法调查还是由被侵权人举证？可见，个人信息保护并不比隐私权高明。

---

[38] 郭瑜：《个人数据保护法研究》，北京大学出版社 2012 年版，第 89-92 页。

[39] 参见前引[38]，郭瑜书，第 89 页。

[40] Stan Karas, Privacy, Identity, Databases, American University Law Review. Volume 52. Issue 2. P. 393-443(2002).

四、重新审视隐私权:一种信息规则

Web2.0 对于隐私权最大的挑战在于,之前很多被认为是正常的行为在大数据时代性质发生了变异,变成了可能侵犯隐私的行为。换言之,大数据极大地扩张了侵犯隐私的深度、广度及严重程度,当然,另一方面也加深了人们对于隐私权的认识,相应地,有必要对原有的隐私权定义做出反思,使之能适应大数据时代的变化。

虽然有人认为给隐私权下定义不可能[41],如 Robert Post。还有人认为给隐私下定义没意义,[42]如 Judith Thompson。但大多数学者还是倾向于给隐私权下定义。在西方历史上出现过六大类有代表性的隐私权定义。

1. 个人独处理论。该理论是 Warren 和 Brandeis 在其著名的《论隐私权》[43]中提出的,他们将隐私权简单地定义为"个人独处的权利",是不可侵犯的人格尊严。然而,这种理论遭到了许多人的反对,因为这个定义实在太过于宽泛了。Anita Allen 对此进行了阐释:"如果隐私权就是个人独处的权利,那么行为人对他人实施的任何具有冒犯性或伤害性的行为都会被看作隐私侵权行为。打他人的鼻子是隐私侵权,偷窥他人卧室也是隐私侵权"。也有人认为 Warren 和 Brandeis 根本就没有给隐私权下定义。[44]

2. 限制接触理论。该理论认为,"隐私权意味着,他人有权决定公众能够在多大程度上了解他人的思想和情感、私人行为和私人事务"[45]。申言之,保护他人的隐私权就是要保护他人免受行为人不受欢迎的接触,无论行为人接触的是他人的身体,还是他人的个人信息,或者行为人仅仅引起他人的注意,这些行为都是不被允许的。[46] 显然,个人独处时的隐私权是最为完全的,但个人独处推演至极致便成了悖论,与世隔绝时讨论隐私权根本就没有任何意义,在此意义上来说,More 的论断是正确的:社会的存在是隐私权的基础,没有社会就没有隐私权。因此,隐私权的范围必须有所限制,但"限制接触理论"并没有给出明确的答案。

3. 秘密理论。该理论认为,"隐私权是指他人享有不被行为人知悉其过去、现在的生活经历以及将来计划的权利"[47]。但是该理论有两个缺陷:一是内容过于狭窄,"秘密理论"只是限制接触理论的一个子集合,不能满足现代隐私权保护的要求;二是过于僵化,将隐私权推向了公开的对立面。按照"秘密理论",信息一旦公开就不再具有保护价值,公共场所的隐私权不受保护。但即便在公共场所,我们也希望隐私权得到保护。

---

41 Robert C. Post, Three Concepts of Privacy, 89 Geo. LJ 2087,2087(2001).

42 *See* Ken Gormley, One Hundred Years of Privacy, 1992 Wls. L. Rev. 1335,1339.

43 Samuel D. Warren & Louis D. Brandeis, The Right to Privacy,4 Harv . L. Rev. 193 (1890).

44 参见张民安主编:《美国当代隐私权研究》,中山大学出版社 2013 年,第 14 页。

45 E. L. Godkin, The Rights of the Citizen, IV-To His Own Reputation, Scribner's Magazine, July-Dee. 1890, at 65.

46 Sissela Bok, Secrets: On The Ethics Of Concealment And Revelation 10-11(1983).

47 Sidney M. Jourard, Some Psychological Aspects of Privacy, 31 Law & Contemp. Probs. 307, 307 (1966).

4. 个人信息的自我控制理论。美国联邦最高法院认为,隐私权就是指他人享有控制与其个人有关信息的权利。[48] 个人信息的自我控制理论也可以视为限制接触理论的子集合,和"秘密理论"一样,也显得过于狭窄。不仅如此,该理论还存在两个方面的缺陷:一是对他人可控制信息的范围没有做出界定,现实生活中很多人都可以看到、听到他人的私人信息,他人也并不乐于接受这样的行为,但他人根本不觉得这样的行为就是隐私侵权行为,这表明该理论与人们心中真正的隐私侵权行为存在较大偏差,关于信息的界定过于宽泛;二是对如何控制也没有明确界定,有人认为个人信息应被视为一种财产权,控制乃是行使信息所有权,这无疑是对控制的曲解。

5. 人格权理论。"人格权理论"认为,保护他人的隐私权就是保护他人人格权的一种具体表现形式。但是,人格权的范围较之于隐私权的范围更大,隐私权属于人格权的一种,但人格权不能等同于隐私权。更为重要的是,"人格权理论"也没有阐明隐私权的本质,"将隐私权看作自治权的一种具体类型意味着隐私权只是他人在道德上享有的自由,若果真如此,隐私权对于他人权益的保障将会变得毫无价值可言"[49]。

6. 亲密关系理论。亲密关系理论认为隐私权对于他人的自我创造很重要,对于人际关系的维持也很重要。根据亲密关系理论,他人享有隐私权意味着他人有权现在行为人接触他人,有权对其信息进行控制。总之,如果隐私权都不保护他人和别人的亲密关系,那么这种亲密关系就不复存在。[50] 但由于亲密关系理论没有对"亲密性"一词进行限定,使得该理论成为了一种宽泛的亲密性含义与只强调狭窄的亲密关系的混合体。

在我国,王利明教授认为"隐私权就是自然人对于自己的私人生活安宁和私人信息安全所享有的权利"[51],实质上属于独处理论和个人信息控制理论的混合理论。张新宝教授则认为"隐私权是指法律赋予自然人的私人生活安宁不被他人非法侵犯和私人信息秘密不被非法获知的权利。同时,隐私权还包括自己能够决定公开自己隐私的范围和他人可以介入自己生活程度的权利"[52]。这也属于独处理论、个人信息控制及自决权的综合理论。

综观上述定义,笔者发现,除我国学者外,国外大多数学者都试图以一元化的理论来定义隐私权,即"通过寻找事物共同特征这一方式"来寻求隐私权的定义,然而,凡是基本能包容大致公认的几种类型的隐私权的定义却往往因为范围划定过于宽泛而包含了不少已经不被认为是侵犯隐私权的行为,比如,"限制接触理论"几乎可以囊括后面的四种理论,但由于其无法就"限制程度"划定具体的界限而流于宽泛;"个人独处理论"固然不存在划定具体界限的问题,但其较之于"限制接触理论"更为宽泛,从限制"个人独处理论"的范围来看,"限制接触理论"的方向是正确的。

---

[48] *See* United States Dep't of Justice v. Reporters Comm. For Freedom of the Press, 489 U.S.749.763 (1989).

[49] Jed Rubenfeld, The Right of Privacy, 102 Harv. L. Rav. 737, 750 (1989).

[50] *See* Robert S. Gerstein, Intimacy and privacy, in Philosophical Dimensions of Privacy.

[51] 王利明:《隐私权的新发展》,载《人大法学评论》2009 年第 1 期。

[52] 张新宝:《隐私权的法律保护》,群众出版社 2004 年版,第 12 页。

然而，为什么包容性越强的定义越容易“失败”呢？或许应该反思的是我们下定义的惯性思维，也就是说，我们认为比较宽泛的所谓“失败”的理论，恰好是最接近问题实质的理论。原因在于，第一，隐私权有着更为丰富的涵义。目前比较公认的论断包括：隐私是一种不可侵犯的人格；隐私是一种特殊利益；隐私是一种自治；隐私和信息的支配有关；隐私是一种私人领域；隐私是限定自我的边界。与之相应，隐私权的次级类型也不少，比如，Prosser 在其《论隐私权》中将隐私侵权行为分为四类：擅自使用他人姓名、肖像或者照片的行为；不合理地侵扰他人安宁的行为；公开披露他人私人事实的行为；公开丑化他人形象的行为等。[53] 换言之，隐私权本质上就是一系列次级权利和利益的组合，这些权利和利益之间或许只有相似性而无绝对的公共性，寻找共同性定义的做法不可避免地会失败。第二，隐私权的定义并不是一成不变的，具体的语境下涉及的隐私权问题也不相同，与习俗、惯例、传统、文化等也有关系。第三，真的需要一个“能且仅能”包含现有隐私侵权类型的隐私权定义吗？套用逻辑学上的术语，该定义的要求为，种概念与属概念的外延应相称、“属差”应尽可能详细确切。事实上，越是这样的定义越没有生命力，因为隐私权的范围是一个动态平衡的范围，有些隐私侵权行为或许随着时间的变化而不再作为侵权行为，而有些则正好相反，从适应性的角度来看，没有必要要求隐私权的定义种概念与属概念的外延应相称、“属差”尽可能详细确切。可见，我们必须转换思路考察隐私权的定义。

Solove 在其《隐私权的概念》一文中指出，“根据 Wittgenstein 的家族相似性理论，除了通过寻找事物共同特征这一方式外，还可以通过其他方式来给事物下定义”。[54] 据此，笔者认为，以相似性来定义隐私权或许是一种不错的选择。大数据时代的一切都可以表现为以数据为纽带的信息，隐私最直观的表现为有关个人的信息，隐私权则表现为个人信息不受干扰。事实上，笔者可以将任何公认的侵犯隐私的行为解释为对信息的干扰。索洛韦伊将侵犯隐私的行为分为：信息收集行为、信息加工行为、信息传播行为及侵犯他人私人事务的行为，[55]前三种不难理解，都是对个人信息的干扰行为，最后一种可以解释为在他人正在形成的信息上添加信息的行为或者使他人意欲形成的信息不能充分表露的行为，这当然也是对他人信息的干扰。据此，各种隐私利益之不远不近的上位概念隐私权，从形式上看，就是个人信息免受干扰的权利。事实上，该定义是“限制接触理论”的引申，但较之更进一步，表现在两个方面：一是将所有接触的形式都转换为信息作用行为，符合大数据时代的特点；二是从效果方面对限制进行界定，只要干扰了他人信息都可能侵犯隐私权。

在笔者看来，大数据时代，必须以一种全新的视角来看待隐私权：大数据时代的隐私权不是即将消亡，而是越来越重要，关乎人们的身份、平等、安全以及信任的建立，从

---

53 William L. Prosser, Privacy, 48 Cal. L. Rev. 383, 389 (1960).

54 Daniel J. Solove, Conceptualizing Privacy, California Law Review, Vol. 90, p. 1087, 2002.

55 Daniel J. Solove, University of Pennsylvania Law Review, Vol. 154, No. 3, p. 477, January 2006, GWU Law School Public Law Research Paper No. 129.

而实质性地影响我们赖以存在这个世界的政治、经济和文化基础;大数据时代的隐私不再被纯粹地当做一种秘密,而是一种处于秘密与完全公开之间的中间状态,在此意义上来说,隐私权不是一种绝对的权利,而是一种相对的权利,是一种信息管理的规则;与其关注隐私权的本体是什么,不如以问题为导向在实践中发现、建立规则,在立法时机并未完全成熟的现阶段,司法先行具有一定的可取性,在司法实践中针对个案确立规则,但必须受到一定的限制,依据一定的原则和共识进行。

总之,国内外的理论和实践表明,试图构建一个"种概念与属概念的外延应相称、'属差'详细确切"的隐私权定义几乎是不可能的,也是没有必要的,构筑隐私权定义的根本目的在于更好地保护法益,因此,只要形式的定义在实践中好用,不必纠缠于如何给隐私权下实质的定义,形式的定义更具有包容性,能更好地解决不同类型的隐私权难于统一的矛盾,给予最大范围的隐私权保护的可能。

五、构建隐私的实质标准:综合衡量

不可否认的是,形式的定义需要实质的标准加以补充,正如德日刑法中的犯罪概念一样,虽作为形式定义,但同时满足三个实质的标准犯罪就可以成立一样。从这个意义上来说,隐私权的判断标准比定义本身更为重要。这里需要指出的是,隐私权的判断标准不同于隐私侵权的规则,前者是实体权利是否存在的标准,而后者则是对实体权利进行处置的规则,二者有重合的地方,前者是后者的前提,但二者不可混淆。

关于隐私权的判断标准,美国通常采用的是"隐私的合理期待"标准,源于美国联邦最高法院在 1967 年的 Katz v. United States[56] 一案中作出的里程碑式的判决,其主要考察行为的三个方面的要素:监视发生地、监视行为的侵扰程度、监视的对象或性质。但该标准主要是针对监视行为或搜查行为的,也就是有关空间的隐私判断标准。

"隐私的合理期待"标准为所有类型的隐私标准的建立提供了线索。所谓合理的期待标准,是指理性的个人认为在案件的条件下他应该享有隐私权,这是一个英美法系中的理性人标准。理性人标准并不是一个主观标准,任何个人的标准都不能作为隐私权存在的标准,而只有那种依据普通人的常识和逻辑都能推论出来的标准才是"隐私的合理期待",可见理性人标准是一个客观标准。在法律领域中,行为总是居于中心地位,对于行为的评价总是根据行为及随附情况共同组成的行为系统来加以评价的,隐私权的判断也不例外,具体而言,是否存在"隐私的合理期待"可以从作用于隐私对象之行为出发加以考察,换言之,须结合行为的方式、目的、结果、对象、范围等进行综合判断。

1. *行为方式的影响*。行为的方式决定行为的性质,是判断行为是否侵犯隐私权的首要依据,也是隐私侵权类型化的基础。大数据因其超强的信息收集、整合及挖掘、预测能力对隐私构成了巨大威胁,很多信息收集行为天然地具有很强的侵袭性,很难为人

[56] 389 U.S. 347 (1967).

们所接受,这类行为中普遍引起人们关注的主要包括以下几种。一是利用高科技的监视行为。比如高空监视、热成像监视及层出不穷的谷歌街景拍摄到不雅照片、犯罪情形等。早先,判断政府机构使用此类高科技行为是否侵犯隐私以公共场所和私人场所作为是否侵犯隐私权的分野,即在公共场所使用此类技术不属于侵犯隐私权,在私人场所则正好相反。但现代科技的发展突破了物理性侵袭的界限,使得区分公、私场所的围墙、房屋等形同虚设,不利于隐私权的保护,因此以行为对象如收集的信息之内容为依据判定是否侵犯隐私成为必然。但若没有公共利益的介入,个人使用此类技术,不管是否造成有形的损害,都属于侵犯了他人的隐私权。由此可见,行为方式对是否侵犯他人的合理隐私期待具有重要意义。二是人肉搜索行为。"人肉搜索"是指"区别于机器搜索(如百度、谷歌之类的搜索引擎)之外的另一种搜索信息方式,是通过集中网民的力量去搜索信息和资源的一种方式,它包括利用互联网的机器搜索引擎(如百度等)及利用各网民在日常生活中所能掌握的信息来进行信息收集的一种方式。"[57]但是,除了极少数具有抗辩理由之外,其中大部分的人肉搜索行为涉嫌侵犯了他人多种类型的隐私权,如扰人安宁及侵犯肖像权、名誉权等。其他一些行为方式和上述两种行为相比则显得没那么令人难以容忍,有些甚至还可以带来一定的好处,比如预测性广告等。

2. *场所之影响*。场所也是判断隐私的重要因素。比如,美国宾州一对夫妇向法院控告 Google 公司,指该公司地图网站可查看其房屋图片,涉及侵犯隐私,并使房价下跌。然而在宾州阿雷格尼郡(Allegheny County)的房地产网站上,也可以见到波林夫妇的房屋图片,却因为那些图片是在公用道路上拍的,"并未擅入私人土地"而未被起诉。[58] 此外,如前所述,高空监视、热成像等表明场所曾与"隐私的合理期待"有关,但还存在另一种影响方式,即特点的场所会减损其隐私期待的合理性。美国联邦最高法院在 O'Connor v. Ortega[59] 一案中对此进行了详细论述。大法官 O'Connor 认为,工作场所的办公运行机制可能会使雇员的隐私期待的合理性大打折扣,即所谓隐私权的消退。

3. *对象之影响*。行为对象对隐私权是否存在也具有相当大的影响。比如,有关个人的信息中,一部分属于一般信息,另一部分属于敏感信息,他人对二者具有的隐私之合理期待是不同的。披露他人的敏感信息可以构成隐私侵权,这很容易理解。敏感信息一般指心智正常之普通人不欲向他人展示之生理特征或情感特征等,"属于人类高度原始的特征,一旦被披露会引起人们的尴尬和羞耻感,如悲伤、痛苦、肉体创伤、精神创伤、裸体、性行为、排尿、排便等都是人类生活中最为原始、私密的一部分,都是人类不可

---

[57] 载 http://baike.baidu.com/view/542894.html? reforce = 人肉搜索引擎 &hold = synstd, 最后访问时间:2015 年 12 月 16 日。

[58] Google Street View 被起诉侵犯隐私 - Google Map 应用 - 上帝之眼—Google Earth[谷歌地球]资讯门户, 载 http://www.godeyes.cn/html/2008/04/07/google_earth_1610.html, 最后访问时间:2016 年 8 月 17 日。

[59] 480U.S.709(1987).

缺少的基本特征"[60],但经过社会之教化,人们都懂得将这些基本特征隐藏起来。[61] 此类信息一旦被披露,无疑会降低他人的人格尊严,造成精神上的创伤。但公开他人的一般信息损害了人们的交往自由和匿名权,如果这些权利受到威胁,人们就会不愿意参与有利于自我发展的活动;此外,匿名权本身对于促进自由表达观点起着关键作用。然而,公开他人一般信息还可能威胁人们的人身财产安全,如 RemsburgV. Docusearch, Inc.[62]一案。此外,他人信息的公开不仅不会提高人们评价他人之能力,反而更可能歪曲对他人的评价。因此,隐私权法对他人一般信息也予以保护。

4. 行为范围之影响。一般而言,即使是对于他人自愿公开的信息,如果传播者超越了他人所意愿的范围,也可以构成隐私侵权。比如,他人在小范围内因交际需要而披露的信息,倘若被听众传播至较大范围,也可能构成隐私侵权。

5. 行为结果。行为结果无疑也是影响因素之一,虽然有些行为的损害不那么明显,或者只是其他侵权行为的预备行为,但某种行为之所以让人们不能容忍,显然是因为其带来的不利后果或者不利威胁,从这个意义来说,行为结果既是判断隐私权是否存在的关键,也是应否给予救济的判断依据。根据汉德公式[63],B < PL 时,(B 代表预防成本,P 代表损失几率,L 代表损害结果转换成的金额),侵权法才有存在的意义。

6. 行为正当目之影响。为了公众的福祉,也不会给他人造成损害,因而可以影响隐私权的存在。比如,基于科研而收集的医疗资料以及人口普查等国家行为等。反之亦然。但即使是正当之目的,对于他人信息的收集与披露也必须限定在一定的范围之内。此外,基于正当目的所搜集之信息,如果未经他人之同意,擅自用作它途,即所谓信息的第二次利用行为也是不能被允许的,例如,通过正当途径获取的信息向信息主体进行电话销售、发送垃圾信息或者其他形式的侵扰性广告等。

7. 限制因素。由于隐私权不是一个绝对的权利,必然要受到很多因素的制约,因而在考察是否具有合理隐私权时应有所限制。第一,文化因素。人是群居的动物,人与人之间的交往本来就是以信息为纽带的,人际交往中相互披露信息被认为是友善和亲密的标志,这种情形下不宜将人际交往中相互披露信息的行为认定为侵犯隐私权。有证据表明,现代人越来越适应这种隐私权逐渐缩小的生活方式。[64] 第二,权衡相关价值,避免"寒蝉效应"。隐私权经常与其他价值相冲突,如与言论自由、国家安全、公共福祉、法律执行、经济创新等相互制约,侵权法应致力于寻求一个适当的平衡点。

---

[60] AnitaL. Allen, Lying to Protect Privacy, 44 VILL. L. Rev. 161. 177(1999).

[61] *See* BrBert, the Civilizing Process 114(edmund Jephcott trans., 1994)(1939).

[62] 816A. 2d1001, 1005 - 1006(N. H. 2003). 本案中,一名精神错乱的男子对 AmyLymn Boyer 非常迷恋,他从一家数据库经营公司购买了 Boyer 的 SSN 和工作场所的地质,并到其工作场所将其杀害。

[63] 参见[美]波斯纳:《法律的经济分析》,蒋兆康译,法律出版社 2012 年版,第 105 页。

[64] *See* Richard A. Posner, Privacy, Surveillance, and Law, 75 U. CHI. L. REV. 245, 249-51 (2008).

六、侵权规则之重构

(一)损害结果应适度扩张

权利的宣示并不等于权利的保护,权利的保护有赖于有效的侵权法制度之建立。大数据时代隐私侵权的扩张,形式上为行为方式的扩张,实质上是损害结果的扩张与多样化。某种隐私侵权类型能否成立,往往依赖于背后隐藏的具体法益是否值得保护,因为,现代侵权法是基于损害-赔偿模式的法律制度,损害结果无疑是侵权法的第一要素,直接关系到被侵权人能否获得法律救济,大数据时代的隐私侵权虽然有其特殊性,但也不应该突破损害—赔偿模式。对于某些损害结果之认定,可以采取某些便宜行事的方式,比如,对于某些特别具有侵袭性的行为,只要一经实施该行为,便可以认定对他人之精神造成损害,而不必拘泥于证明其精神损害的具体表现。鉴于此,美国不少学者致力于隐私损害的研究,试图得出一个更具实践性的结论,[65]然而,欧洲的学者则倾向于认为隐私权是一种基本人权而拒绝对隐私损害结果进行讨论。[66]

在大数据时代,隐私侵权出现了一系列新的损害形式,突破了传统的隐私侵权损害结果的范围,有些损害与侵权行为之间的因果联系更为松散,这些损害能否得到承认呢?在笔者看来,隐私权的损害结果不应仅仅局限于所谓的精神损害,其范围应扩张,对下列损害结果应予以承认。

其一,扩张无形损害的范围。大数据时代隐私侵权的后果往往十分隐秘和不那么明显,有些特殊的损害结果应予以承认,比如,应将大数据导致的不公平、不平等及歧视等视为隐私权损害的结果。正如 Polonetsky 所指出,大数据时代的信息收集过程越来越多地涉及到公正、平等权利,而这些即使理论上区别于其他隐私权益,但绝不意味着不如其他隐私权益重要。[67]此外,Dwork 和 Mulligan 则分析了商家基于地理位置和消费者当时的心情而导致的价格歧视的机理。[68] 事实上,随着大数据时代对基因信息、健康信息等越来越重视,就业歧视和保险歧视等只会与日俱增,这种无形的损害往往令被侵权人不明就里,危害极大,也应该视为隐私侵权的后果予以救济。然而,我国目前虽然禁

---

[65] *See* Helen Nissenbaum, Privacy in Context: Technology, Policy, And The Integrity of Social Life 1 - 4 (2010); Westin, supra note 157, at 42; Ruth Gavison, Privacy and the Limits of the Law, 89 YALE L. J. 421, 422 - 24 (1980); William L. Prosser, Privacy, 48 CALIF. L. REV. 383, 422 - 23 (1960); Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, 4 HARV. L. REV. 193, 214 - 20 (1890).

[66] *See* Org. for Econ. Co-operation & Dev. [OECD], Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, OECD Doc. C(80)58/FINAL (Sept. 23, 1980) [hereinafter OECD Guidelines], available at http://www.oecd.org/internet/iecon omy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

[67] *See* Omer Tene &JuloPolonetsky, Big Data for All: Privacy and User Control in the Age of Analytics, 11 Northwestern Journal of Technology and Intellectual Property 239 (2013).

[68] *See* Cynthia Dwork & Deirdre K. Mulligan, It's Not Privacy, and It's Not Fair, 66 STAN. L. REV. ONLINE 35, 36 - 38 (2013).

止就业歧视已经引起各方广泛的关注，但就业歧视仍普遍存在，而提出诉讼的不到1%，[69]显示公众对禁止就业歧视这种权利的认同感不强，即使有些“就业歧视”能获得法律上的救济，其依据多是以违反了劳动法等相关法律为依据的，用人单位侵犯的是平等就业权而非隐私权，侵权主体也不是隐私信息的提供者。

其二，扩大经济损害的范围，期待利益也可以考虑。数据泄露导致的冒用身份、诈骗等往往给受害人造成严重的损失：侵权人可以利用他人的身份转移他人银行账户的存款；利用他人身份进行贷款担保或者信用卡消费；甚至有人冒用他人身份享受医疗健康服务从而给受害人留下巨额医疗费用；身份盗窃会破坏他人的信用评价而导致就业能力受损、贷款资格受损。即使这种信用可以修复，也需要花费大量的财物，在美国有人估计信用修复的平均耗费为 $5,720。[70] 在我国，最为典型是电信诈骗。电信诈骗不仅给直接受害者带来财产甚至生命损失，也加剧了人与人之间的不信任，增加了社会运行成本，损害社会信任的基石。所有这些损害，都应该算作侵权导致的经济损害。当然，上述冒用身份及诈骗等行为，往往因为直接行为人已经构成其他侵权行为甚至犯罪，可以不经过隐私侵权来救济，但对于网络营运商单纯泄露信息的行为，也可以令其单独或者连带负隐私侵权的责任。

其三，扩大人身损害的范围。如前所述，信息泄露也可能导致被害人被抢劫、强奸甚至杀害。固然，抢劫或强奸、杀害等行为有其直接行为人负相应的刑事责任甚或附带民事责任，但美国曾有案例判决信息泄露者承担侵权责任，这种做法值得借鉴。

其四，对于无形损害，可以采取推定损害存在的方法。大数据时代的隐私侵权获得救济的主要障碍之一是难以证明损害结果，比如，社会评价降低的范围和程度很难进行量化分析，与之相应的是索赔金额的合理性，经济损失的数额难以量化；若以患有精神疾病的诊断证明作为索要较大数额的精神损害赔偿的依据，则证明精神病与侵权行为的因果关系更是十分困难。对于此类无形损害，可以根据侵权内容的点击率、转载率来间接地推定损害结果的严重程度，并且这种推定不能反驳。但张新宝教授认为“推定的损害事实是指人格方面的损害或者说外部名誉的损害，而不包括对精神损害之存在的推定。作为内部名誉损害的精神损害是不能推定存在的”[71]。事实上，一般而言，精神损害与传播的深度与广度呈正向相关关系，依传播的深度与广度推论精神损害之存在并无不妥，但推论出精神损害已达到呈现精神症状的程度却未必妥当，在此意义上张教授的观点是正确的，但并非只有精神损害达到事实上出现精神症状的程度才可能获得救济，只要足以产生精神上的压力即可，因此，以传播的深度与广度推定精神损害的存在并无不妥。

---

[69] 2013 年人力资源蓝皮书：就业歧视仍较普遍，载 http://www.china.com.cn/news/txt/2013-10/10/content_30249267.htm，最后访问时间：2015 年 5 月 25 日。

[70] John Leland & Tom Zeller Jr., Technology and Easy Credit Give Identity Thieves an Edge, N.Y. TIMES, May 30, 2006, http://www.nytimes.com/2006/05/30/us/30identity.html.

[71] 张新宝：《侵害名誉权的后果极其民事救济方式探讨》，载《法商研究》1997 年第 6 期。

(二)因果关系的判断宜采"条件说"

扩大损害的范围还必须要解决一个理论上的难题,即有些损害与信息泄露行为只存在条件关系,按照我国所采用的原因说则因果关系能否成立尚有疑问,笔者建议在认定因果关系时采用条件说。但这又会引发一个问题,为什么同在侵权法的领域中,因果关系的认定却采用不同的学说。侵权法不过是一种平衡各种利益工具,只要能有效地实现各种利益的平衡,可以在不同类型的案件中采取不同的认定标准,我国侵权法中存在的特殊侵权如医疗侵权等正是这种做法最好的注脚。《刑法修正案九》也为条件关系也是因果关系提供了理论支撑,其中的"情节严重"有论者在立法修改建议中解读为:导致被害人人身伤害或死亡的、严重影响背后人名誉等。[72] 对于此类案件,因果关系的判定可才用条件说,只要涉及本案的任何一个环节之主体,均可以作为侵权主体而被追诉。

(三)部分网络侵权可采过错推定原则

按照我国通常的侵权行为构成要件理论,要认定隐私权侵权责任,需采取过错归责原则,即必须要存在具备侵犯隐私权的行为并造成损害事实,损害行为和损害事实之间有因果关系,而且侵权人还必须是有过错。[73] 然而,在大数据时代,网络侵权有时候连侵权的主体都找不到,更遑论证明其存在过错了,这意味着大量的侵权案件因无法证明过错的存在而得不到救济。有学者收集的 28 例隐私侵权案例中就有 6 例因无过错抗辩而未获救济。[74] 由于诉讼双方诉讼能力上的悬殊,原告起诉网络运营商获得救济的机会很小。为改变诉讼双方能力上的不平衡,采用一些特殊类型侵权如医疗侵权中已经广泛使用的过错推定原则往往是一种有效的选择。

所谓过错推定原则,是指在法律有特别规定的情况下,基于损害事实的客观存在,推定加害人行为有过错并因此而承担赔偿责任的原则。对于网络运营商等数据控制者适用过错推定原则是基于以下理由:其一,不少网络行为本身就隐含着高度的危险性,往往会给受害人带来严重的危害,使他人的人身和财产安全受到极大威胁。比如数据的收集者将敏感信息泄露给身份窃贼等犯罪分子。其二,信息一旦被收集就处于收集者排他性的控制之下,从诉讼便利和经济的角度来看,让受害人发现信息收集、加工、存储、利用过程中的过错是十分困难的。其三,大数据带来的隐私损害不是被害人自己谨慎行事就能避免的。大数据时代,个人隐私变得十分脆弱,很多时候甚至都不知道自己的隐私权被侵犯,更谈不上有意识地避免了。即使在同意-选择的模式中,也会因为害怕不同意便失去服务的机会而事实上被强制而选择同意。其四,从功利的角度来看,过错推定原则可以促进网络营运商和信息收集者强化安全意识,为网络安全营造一个良好的环境,消除消费者、用户的顾虑,促进隐私和经济创新的平衡。

---

[72] 参见张磊:《司法实践中侵犯公民个人信息犯罪的疑难问题及其对策》,载《当代法学》2011 年第 1 期。

[73] 参见张新宝:《侵权责任法》(第 2 版),中国人民大学出版社 2010 年版,第 29 页;杨立新:《侵权责任法》(第 2 版),法律出版社 2012 年版,第 77 页。

[74] 参见叶名怡:《真实叙事的边界——隐私侵权抗辩论纲》,载《中外法学》2014 年第 4 期。

当然,为了不过分加重运营商的责任而影响互联网的发展,过错推定原则只在实际的损害已经发生时才能适用。即使某一行为看起来具有相当的危险性,达到侵犯隐私权的合理性怀疑的程度,也不能据此而推定损害的成立。比如,美国法院曾驳回了原告因数据泄露导致遭受信用卡盗窃的危险性增加的案例。[75] 但对于数据泄露导致精神损害等无形损害恐将引起争议。

同时,过错推定原则也并非针对所有的运营商适用。根据控制力理论,网络运营商对网上信息具有控制能力,不同的运营商具有不同程度的控制力,因而应区分对待。

网络接入服务提供商(Internet access provider,简称 IAP)是为用户提供网络连接、IP 地址分配、解析和路由等服务的运营商。网络接入服务提供商的作用仅限于为用户提供网络通道,其本身既不提供网络信息,也不对线路中传输的网络信息加以存储、编辑或监控,因此,除非其主动编辑、修改信息等,否则,原则上不承担直接侵权责任,也不承担因审查而过失导致的隐私侵权责任,因为从海量信息中进行筛选、监控的代价十分巨大且不现实。因此,对此类运营商不适用过错推定原则。

网络内容服务提供商(internet content provider,简称 ICP)是指为用户提供各种信息浏览与阅读服务,以及搜索引擎等链接服务的网络服务提供商。由于其在信息传递过程中最为主动,创作、收集、整理、编辑信息并在网络上发布是其主要工作,所承担的义务也更多,是侵权行为发生的主要环节,对此类运营商应适用过错推定原则。

网络平台服务提供商(internet platform provider,简称 IPP)是指为用户提供网络交流平台的网络服务提供商。由于其服务内容主要是交互形式为上网用户提供信息发表平台,处于中间者的地位,负有合理审查及协助调查的义务,合理审查义务包括人工审查和技术审查两种,人工审查是通过人工浏览对明显反动、侵害他人名誉权和隐私权的帖子进行审查,并负有立即删除的义务。由此可见,网络平台上隐私侵权行为之发生,往往与服务提供商疏于审查有关,因此一旦发生隐私侵权的行为并造成一定的损害,就可以推定其过错的存在。

(四)隐私侵权的救济方式

在大数据时代,隐私侵权的损害结果已经发生了深刻的变异,传统的救济方式还能起到应有的作用吗?

根据侵权行为的损害后果之性质与责任方式的对应性的要求,侵害财产权的侵权行为造成受害人财产损害的,加害人一般应承担财产性质的侵权责任,如赔偿损失、返还财产;侵害人格权的侵权行为造成受害人名誉等受到损害的,加害人一般应当承担人身性质的民事责任,如消除影响、恢复名誉和赔礼道歉等。但这只是一般性的要求,除了性质的对应性要求之外,还应该有程度的要求,如我国刑法中的罪、责、刑相适应原则。由于大数据时代的隐私侵权所导致的损害强度大幅提升,相应地,救济方式也应该有所改变。对于网络隐私侵权的救济方式,可以从两个方面进行改进。

---

[75] *See* Daniel J. Solove, Understanding Privacy 177 (2008).

一是对消除影响、恢复名誉和赔礼道歉的方式和程度作出规定。一般说来，消除影响、恢复名誉都应当是公开进行的，其内容须事先经过人民法院审查。恢复名誉、消除影响的范围，一般应当与侵权行为造成不良影响的范围相当。[76] 这意味着，对消除影响、恢复名誉的媒介应与侵权行为的媒介相当，且存续的时间不能过于短暂，点击率应达到一定的程度。否则，很难起到消除影响、恢复名誉的作用。

二是对网络隐私侵权引入惩罚性赔偿。大数据时代隐私侵权在各个方面都发生了变异，传统的补偿性损害赔偿已经不能满足隐私保护的需要。基于以下原因，应该引入惩罚性赔偿。第一，个人信息价值的分享理论决定了对营运商、信息的利用者应采取惩罚性赔偿原则。虽然说大数据可能最终惠及每个人，但从当前的实际情况来看，作为信息源泉的个人没有在其中真正得到实惠，现阶段真正赚钱的是少数信息控制着和利用者，比如营运商和广告公司等，他们在享有更多权益的情况下，理所当然应承担更多的义务。第二，传统补偿性赔偿预防作用不足。网络服务商在网络侵权时通常会为了获取巨额的财产利益而铤而走险，往往抵消了对侵权后果承担损害赔偿的恐惧，补偿性赔偿无法抑制侵权冲动。第三，维权成本比较。侵权法之构造当然应考虑社会成本的消耗问题。相比于网络营运商和信息的控制者、使用者，普通用户甚至有时候连发现被侵权的机会都没有，更不用说收集足够的证据而获得救济了，能力强者应当承担更多的责任。况且，真正被发现并起诉的侵权行为只是实际存在的侵权行为之极小一部分，对于营运商等来说，根本没有威慑力，以至于其怠于保护用户之隐私。

Abstract: Web2.0 marks the arrival of the era of big data, also means that the arrival of the privacy crisis: it very easy to find the privacy infringement, common; Becoming more secretive behavior mode; Nature is more difficult to determine; Results degree of diversification and more serious. A cause and effect relationship between behavior and the result is more loose. China's traditional way of indirect privacy has seriously lagged behind The Times. For expanding the possibility of privacy tort relief, it is necessary to construct a tort rules: clear privacy protection rather than personal data protection as the basis of route; Take the form of privacy definition and essence of the judgment standard of combining the method determines the existence of the privacy interests; To expand the scope of privacy harmful consequences; For fault presuming principle in order to increase the possibility of this party won.

（责任编辑：李小明）

[76] 参见最高人民法院《关于审理名誉权案件若干问题的解答》（1993年8月7日）。