doi:10.16060/j.cnki.issn2095-8072.2019.05.006

网络服务提供商泄露个人信息侵权责任问题研究

李 磊

（上海对外经贸大学法学院，上海 201620）

摘 要： 网络服务提供商是获取和保有个人信息的最重要主体之一。《民法总则》第 111 条对其设定了对个人信息的安全保障义务，包括一般性义务和阶段性义务。义务内容可结合对相应法律法规的解释得出。网络服务提供商违反该义务应承担侵权责任。在司法适用中，需明确过错的认定和赔偿责任承担方式。违反安全保障义务是“过错”的事实构成，具体构成要件应包括危险开启、必要性和可期待性。“过错”的司法认定可依次考虑成文法规范、行业通行准则、同样错误再犯和公共政策一般原则加以确定。在责任承担方面，对比“通知—删除”模式和“相应的补充责任”模式，前者虽为侵权法中的网络侵权条款，但并不适合违反安保义务的模式，后者更适合。

关键词： 安全保障义务；网络服务提供商（ISP）；个人信息保护

中图分类号： D923.7 **文献标识码：** A **文章编号：** 2095－8072(2019)05－0062－11

《中华人民共和国民法总则》(下称《民法总则》)第111条规定：“自然人的个人信息受法律保护。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，不得非法收集、使用、加工、传输他人个人信息，不得非法买卖、提供或者公开他人个人信息。”此即在规范意义上明确，《民法总则》将个人信息的保护建构在对个人信息的获取者(含保有者、控制者、处理者、使用者，下同)课以对个人信息的安全保障义务的基础上。在诸多获取个人信息的主体中，网络服务提供商(Internet Service Provider，下称ISP)是十分重要的一类。[①]ISP是向网络用户综合提供网络信息业务和增值业务的运营者，其承担着向整个社会提供网络内容服务的重任。[②]有学者讨论ISP与其掌握的个人信息的关系时，以四个特性加以概括：与公众生活的密切联系性、个人信息的易得性、个人信息的易泄露性和个人信息泄露损失的严重性。故对ISP与其掌握的个人信息之关系问题进行民法上的分析十分必要，而现实中已经发生的案件也呼唤民法对ISP泄露个人信息后的侵权赔偿问题予以有效回应。

① 亦有学者以“平台”为对象加以研究。本文认为ISP是“平台”的运营主体，平台是ISP的“前台”。因此ISP应是真正的权利义务主体，也是责任承担主体。此处的“网络服务经营者”类似于《电子商务法》中的电子商务平台经营者,即在电子商务中为交易双方或者多方提供网络经营场所、交易撮合、信息发布等服务，供交易双方或者多方独立开展交易活动的法人或者非法人组织。本文未采用”电子商务平台经营者”之称谓，主要因为《电子商务法》的适用范围较窄，不包括“金融类产品和服务，利用信息网络提供新闻信息、音视频节目、出版以及文化产品等内容方面的服务”的提供者。

② 由于政府及事业单位的非营利性以及责任承担的特殊性，其作为网络内容提供者而造成个人信息泄露的法律责任问题不在本文讨论的范畴之内。

该案基本案情如下：原告通过被告开办的订票网站订机票但其信息被第三方盗取，信息盗取人给原告发了一个短信告知其飞机航班取消的假消息(实际没有取消)，导致原告未能按时乘机。[①]原告起诉被告，要求赔偿损失，公开赔礼道歉。

审理过程中，双方争议焦点聚集于：(1)第三人通过网络技术侵入被告的网络平台窃取了原告信息，对此被告的“过错”如何认定？(2)如果被告应承担侵权责任，应依何规则承担？原告在举证中并未明确指出被告有过错的理由，只是认为原告的信息泄露系被告对个人信息保护不力所致。而被告则认为其已经尽到了对个人信息的安全保障义务，没有过错。二审法院在判决中认为被告是否有过错十分重要，但在过错的认定上却轻描淡写，其判决书写道：“而本案泄露事件的发生，正是其疏于防范导致的结果，因而可以认定被告公司具有过错，理应承担侵权责任”，并最终判决被告败诉，但仅支持了赔礼道歉，未支持赔偿损失的诉请。被告败诉后不服，又提起了再审，并在再审理由中认为“本案属于一般侵权纠纷，应适用过错责任原则，二审判决仅依据信息泄露的客观结果即当然认定我方具有过错，实质对我方适用了无过错原则，显属错误”。显然，法院对被告过错的认定难以让人信服。而在责任承担方面，法院的判决更有逃避责任之嫌。由此可以看出，司法实践中对ISP泄漏个人信息案件的审理，存在着过错认定和赔偿责任承担方式确定两个问题。本文不揣端陋，对上述问题作一探讨。

一、责任的前提：ISP对个人信息负安全保障义务

规范分析可见，《民法总则》第111条并未采用“个人信息权”理论，[②]即并未将个人信息的保护建构在“个人信息权”的基础上，而是采取了对信息的获取者(保有者)课以对个人信息的安全保障义务的方式。本文认为，采用此路径的优点在于：1.可以避开理论争议，以解决问题为导向，即避开以“个人信息权”为核心的“新型权利保护论”与美国法上的“隐私权”保护论的争论。前者在《欧盟通用数据保护条例》中得以全面的展现，而后者则长期存在于美国法的一系列成文和判例法中。[③]《民法总则》这一立法路径，在避开理论争议的同时实现了有效保护，不失为一种务实的做法；[④]2.与其他立法有效衔接，为司法适用提供可行之路。从目前有关个人信息保护的法律看，除《民法总则》第111条外，最主要的有五个。[⑤]其中最重要的是《网络安

① 庞理鹏与北京趣拿信息技术有限公司等隐私权纠纷(2017京01民终509号)。

② “个人信息权论”：此种观点认为，个人信息主要体现的是一个人的各种人格特征，故个人信息权是一种新型的具体人格权。代表学者有王利明教授，齐爱民教授等。

③ 美国法中所称隐私与大陆法中的隐私内涵颇为不同：在美国，隐私权被作为一种门户概念——一扇通往所有潜在的人权的大门，外延很广，足以涵盖超出隐私范畴的人格利益、姓名、肖像等。参见：高圣平. 比较法视野下人格权的发展——以美国隐私权为例[J]. 法商研究, 2012(1): 32–37.

④ 有关个人信息的保护方式的理论争议，国内比较有代表性的有以下三种观点：王利明教授认为应当在民法典“人格权编”中加以详细规定；而张新宝教授认为在民法典“人格权编”中不应该详细规定对个人信息的保护，而应该专门制定“个人信息保护法”加以保护；张平教授则认为，当前对于个人信息法律问题的法理论证尚存诸多问题，故制定“个人信息保护法”的条件尚不具备，可以立足于《网络安全法》及其他一些管理型规定，通过法解释学方法解决个人信息保护问题。

⑤ 这五部法律规范分别是：1. 2012年12月28日全国人大常委会通过的《关于加强网络信息保护的决定》相关规定；2. 2013年修订的《消费者权益保护法》相关规定；3.《侵权责任法》相关规定；4.《中华人民共和国网络安全法》；5.《电子商务法》相关规定。

全法》，该法作为我国第一部以“网络安全”为调整对象的立法，从保障网络产品和服务安全，保障网络运行安全，保障网络数据安全，保障网络信息安全等方面进行了较为全面的制度设计。该法第10条规定：“建设、运营网络或者通过网络提供服务，应当依照法律、行政法规的规定和国家标准的强制性要求，采取技术措施和其他必要措施，保障网络安全、稳定运行，有效应对网络安全事件，防范网络违法犯罪活动，维护网络数据的完整性、保密性和可用性”，同时该法以较大篇幅从维护网络安全的角度规定了ISP应当履行的义务。[①]此外，《电子商务法》第23条、第24条及第30条均规定了电子商务经营者(平台经营者)需遵守有关个人信息保护的法律法规规定，履行保护个人信息的义务。以上条款从内容上既未设定“个人信息权”，亦未走“隐私权”之路，而是均采用了为个人信息采集者、保有者和使用者等主体设定安全保障义务的做法。这既与《民法总则》第111条在立法技术上相协调，又为该条在司法适用上提供了解释和适用的“便利”，尤其在体系化解释上可以相互“引用”，相互印证。[②]

ISP的安全保障义务在性质上是一种危险防免义务，义务人应当积极采取适当与合理的措施对网络服务过程中的危险予以控制或尽可能地降低危险发生的可能性。[③]从我国当前立法看，该义务无法为现行法律中的安全保障义务所完全涵盖。《侵权责任法》中虽有安全保障义务，但该条所规定的安全保障义务适用范围较窄，仅适用于“宾馆、商场、银行、车站、娱乐场所等公共场所的管理人或者群众性活动的组织者”，这显然未涵盖网络社会的各类主体。而且ISP的安全保障义务内容不仅要求其保障特定个体的信息安全，防止特定侵权行为的发生，更是要求其对整体风险进行防控——因为网络空间是一个连续的整体，例如在个人信息收集阶段要求ISP使用确实有效的技术保护措施，如高效安全的防火墙软件等，这是以风险控制为目的的义务内容而非针对特定侵权行为的义务内容。那么具体应如何划定义务的合理范围？如何明确义务适用范围的限度？

显然，无论是《民法总则》第111条，还是《侵权责任法》以及全国人大常委会通过的《关于加强网络信息保护的决定》，均未明确给出安全保障义务的内容，故从法律解释角度而言，须结合《网络安全法》和《消费者权益保护法》相关条款进行，适当参考其他行政法规、部门规章等，并结合行业规范以及域外立法经验。本文认为，ISP对个人信息的安全保障义务可以分为一般义务和阶段义务两部分。其中一般

① 该法其他相关条文亦将在下文中适当加以讨论。

② 其他一些直接规定个人信息保护的零星立法主要包括(但不限于)以下规范:《中华人民共和国护照法》、《中华人民共和国身份证法》等。《护照法》第12条第3款规定：“护照签发机关及其工作人员对因制作、签发护照而知悉的公民个人信息，应当予以保密。”第20条规定：“护照签发机关工作人员在办理护照过程中有下列行为之一的，依法给予行政处分；构成犯罪的，依法追究刑事责任：……(五)泄露因制作、签发护照而知悉的公民个人信息，侵害公民合法权益的……”《身份证法》(2003年6月28日通过，2004年1月1日实施)第6条第三款规定：“公安机关及其人民警察对因制作、发放、查验、扣押居民身份证而知悉的公民的个人信息，应当予以保密。”第19条规定：“人民警察有下列行为之一的，根据情节轻重，依法给予行政处分；构成犯罪的，依法追究刑事责任：……(五)泄露因制作、发放、查验、扣押居民身份证而知悉的公民个人信息，侵害公民合法权益的。”另外，还有一些法规、规章也有零星规定。其中较为完整的是中国人民银行的《个人信用信息基础数据库管理暂行办法》(2005年6月16日通过，2005年10月1日起实施)，该办法对个人信用信息的收集、处理、利用、流通等作了较为详细的规定，是一部较为完整的专门领域的个人信息保护办法。但该办法适用面较窄，因此在法院司法适用中作用有限。

③ 刘召成. 安全保障义务的扩展适用与违法性判断标准的发展[J]. 法学, 2014(5): 69–79.

义务是指ISP在收集、储存、利用个人信息的全过程中均需履行的义务。一般义务的具体内容可以通过上述法律(含行政法规、规章)相关条款确定。其中最为全面的当属《网络安全法》第三章第一节“一般规定”中的内容。根据该节内容，可以将ISP对个人信息的一般安全保障义务总结为“技术性保障义务”(第21条、22条第1、2款，23条和25条)，即ISP对其收集、存储和利用的个人信息的全过程之安全须提供技术上的保障。《消费者权益保护法》第29条和《个人信息保护法(草案)》第9条亦有相关规定，但从内容看仍属于宣示性质，不涉及具体义务内容。

阶段性义务则具体包括以下几点：

1．信息收集和存储阶段的告知和谨慎处理义务。告知义务着眼于禁止ISP以不符合法律规定的形式收集储存以及传输用户个人信息，要求其收集个人信息必须告知本人并获得同意(《网络安全法》第22条第3款、第41条第1款)，并采用适当的管理和技术措施，防止数据在储存和传输阶段遭受未经授权的访问、披露、篡改和损毁，避免来自第三人或其他用户造成的损害。不合法，不合规的搜集、存储不仅本身是对个人信息的侵害，而且可能存有安全漏洞，为第三方觊觎甚至侵犯。谨慎处理义务具体包括：第一，在经营范围内收集的个人信息仅可用于与该信息相关的经营业务，不得用于与此无关的其他用途。[①]第二，ISP应当以个人信息被侵犯的可能性最小化的方式使用个人信息。[②]第三，ISP应严格保密所使用的个人信息，不得泄露、出售、或非法向他人提供。[③]第四，ISP不得保有超出存取或其他使用期限的个人信息。[④]

2．信息加工处理阶段的诚信义务。为了更好地利用个人信息，在收集信息后，ISP可能要对于个人信息进一步加工处理，如进行筛选、分类、研究，以期获得符合利用条件的信息形式。诚信义务要求行为人发自内心地为对方着想，真心诚意完成信息加工工作。显然，诚信义务的要求高于谨慎义务。这是源于“加工”环节的风险特点。个人信息的加工环节风险主要存在于两个方面：一是自行加工处理中泄露；二是委托第三方加工处理时泄露。加工环节风险的特点在于：除了和其他环节相类似的泄露外，还可能因为错误加工导致信息主体(权利人)的个人信息被改变、错配，从而引发风险；以及委托加工时因未尽到合理的选任和指示义务，致受委托方在加工过程中产生的各种风险。可以看出，信息加工环节风险发生的可能性高于其他环节，还存在信息被改变、错配的可能性。故该环节应当被课以更高要求的诚信义务。此义务包括：第一，在自己加工处理过程中需尽到最大谨慎处理义务，尽量保证个人信息不外泄；第二，负责收集信息的ISP不得擅自将个人信息加工工作委托给第三方。如确有必要委托第三方加工，应将数据做特殊处理，并且尽到审慎选择义务，且应当及时告知用户；第三，对第三方加工的过程和结果应尽到最大关注义务。[⑤]

①《网络安全法》第41条、欧盟《通用数据保护条例》(下称GDPR)第5条1(b)及后续相关条文。
② GDPR第5条1(c)及后续相关条文。
③《网络安全法》第45条。
④ GDPR第5条1(e)及后续相关条文。
⑤《网络安全法》第42条、GDPR第5条1(c)及后续相关条文。

3. 信息泄露后的及时补救、告知、警示以及报告义务。《网络安全法》第42条第2款规定："网络运营者应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失。在发生或者可能发生个人信息泄露、毁损、丢失的情况时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。"告知义务指在得知个人信息泄露后，ISP应立即通知受害用户相关情况。告知的对象一般指个人信息所指向的主体。告知义务的具体内容包括受害信息的范围、信息受害的时间与方式、ISP的相应对策与补救措施等。[①]警示义务一般伴随告知义务一起履行，主要是警示遭泄露的个人信息所指向的主体，提醒其防范可能遭受的损失等。报告义务则要求ISP在信息泄露后第一时间向主管部门报告泄露情况，此报告应尽量做到准确、完备。[②]

二、归责的关键：过错之认定

理论上"过错"包含故意和过失两个内容，但从违反安全保障义务之"过错"而言，则一般仅包括"过失"，此为民法学界之共识，无须再行论证。且若ISP对个人信息"泄露"主观上是"故意"，如故意出卖、盗取个人信息，则其过错十分明显，亦无需过多论证。因此，下文中如无特别说明，对"过错"的讨论仅包括"过失"，不包括"故意"。

德国民法理论上，安全保障义务(德国法上称作"安全交往义务")较为特殊。其一开始并未反映在《德国民法典》中，而是通过几个判例得以确认。该义务的目的在于保护《德国民法典》第823条第1款之法益，使其免受不作为的侵犯。[③]目前，对该义务的违反所导致的责任，其请求权基础一般仍为德国民法第823条第1款，即过错责任，而将违反安全保障义务作为过错责任的事实构成。亦即，确认ISP是否存在"过错"，须从构成上判断其是否违反了对个人信息的安全保障义务。根据德国民法理论，构成违反安全保障义务一般要从主体是否是危险的开启者、法益是否具有保护的必要、主体是否采取了必要的措施(必要性)、主体采取的措施是否是可期待的(可期待性)四个方面进行分析。[④]其中，个人信息作为一种法益，其应被保护的必要性已无须论证，本文就其余三点做一讨论。

1. ISP作为个人信息的获取者，亦是危险的开启者，有义务控制此危险。[⑤]开启、维持或主导社会交往之人应当积极采取适当与合理的措施对交往中的危险予以控制或

① 此处，域外立法亦可借鉴，如《韩国个人信息保护法》要求个人信息处理者应当立即通知受害的信息主体下列内容：泄露的个人信息种类、个人信息何时以及如何泄露、信息主体可以做的任何减少因个人信息泄露造成的可能损失的信息等。参见：于冲. 域外网络法律译丛. 民商法卷[M]. 北京：中国法制出版社, 2015:75.

② 于冲. 域外网络法律译丛. 民商法卷[M]. 北京: 中国法制出版社, 2015:75.

③ [德]埃尔温·多伊奇. 德国侵权法：侵权行为、损害赔偿及痛苦抚慰金[M]. 叶名怡, 温大军, 译. 北京: 中国人民大学出版社, 2016: 122.

④ [德]埃尔温·多伊奇. 德国侵权法：侵权行为、损害赔偿及痛苦抚慰金[M]. 叶名怡, 温大军, 译. 北京: 中国人民大学出版社, 2016: 第120–121页。

⑤ 危险开启理论是传统的安全保障义务理论之一，在现代商业社会中，通讯以及交通等科技的发展使得人与人之间的交往更加频繁而有深度，较之传统社会，现代人类更倾向于相互依赖以及相互影响的生活方式。在此大前提之中，每项社会交往的开启都会对他人产生一定影响，包括其中潜在的危险也会对他人产生的负面影响。因此每个开启社会交往之人都应适当注意相关人员的安全，安全保障义务正源于这一理念。参见: 刘召成. 安全保障义务的扩展适用与违法性判断标准的发展[J]. 法学, 2014(5): 69–79.

尽可能地降低危险发生的可能性。网络技术的发展一方面极大地丰富和便利了人们的生活，但另一方面也致使侵害个人信息可能性大大增加，手段也愈发多样化与专业化，个人信息在网络空间中的风险随之攀升：木马程序入侵，黑客攻击安全漏洞都是常见的方式，对于普通用户而言不仅难以察觉，更无从有效进行防范。相较于普通用户，ISP在此种高风险的社会交往中既是交往的主导者，亦是个人信息被侵犯的危险实际开启者：用户虽然是网络交往的主体，但却难以成为网络社会主导者。

网络社会的核心资源是信息，而ISP利用专业技术手段运营其网络平台、系统，事实上掌握了网络社会的信息制造、储存、加工和传播。普通用户既无法了解后台操作状况，更不可能参与上述操作。用户也正是在接受和使用网络内容服务时主动提供或被动地被收集了个人信息，从而面临危险。而个人信息的盗取者也正是针对ISP的信息存储功能进行的攻击和窃取行为。因此个人信息泄露危险的开启者正是ISP。

2．措施的必要性是指为了控制危险，危险开启者应采取必要有效措施。此处的必要性是指一种最低限度的必要性，即控制危险必须要做到的措施。比如，交通管理部门必须保证交通信号灯正常工作，而无法保证交通时时畅通；乡村道路两旁有树摇摇欲坠，即将倒伏，相关部门必须及时加固，保证其不倒伏，但却不必保证树的生长必须朝向一定的形状，等等。ISP作为个人信息泄露这一危险的开启者，可能因采取的措施不够有效，未达到保护个人信息不泄露的必要限度而违反安全保障义务。必要性的判断，既基于客观的规范，也可能是基于判断者的主观经验，以交易观念为基础，即法官基于其生活经验和对措施必要性的理解所做的判断。

3．措施的可期待性是指要求ISP提供的安全保障措施应是可期待的，即在经济上是可行的。反过来，如果一种安全保障措施在经济上是可行的，但ISP未采取，则可能构成对义务的违反。这种“经济上的可行”并非简单地指在技术上能够实现，而是从理性人的“成本收益”分析上是可行的。

“收益”不仅与义务人的收入(或可预防的损失)大小有关，而且也应与危险的大小密切相关。比如我国某经济不发达城市，冬季常年大雪，若此时要求地方政府为保证道路畅通无积雪而不断使用较为昂贵的“绿色”化雪剂，此要求显然缺乏可期待性。但在积雪影响交通时若要求在危险处安放警示标牌，并安排一定警力疏导交通，应该属于“可期待”的范畴。此时若不履行上述义务，就可能违反安全保障义务。

政府活动受到预算限制，不可能不考虑成本与收益。ISP并非政府，作为市场主体，其行为更要受市场理性支配，但理性不等于可以为了利润而不作为。在可期待的范围内，义务主体仍需承担其应承担的义务。

理论上的构成要件需落实到司法的具体判断依据和标准上。在司法上，判断一起ISP在个人信息泄露事件是否违反安全保障义务，可以有以下依据：

首先是基于成文法明确的义务性或强制性规定。成文法是我国调整和规制网络社会的基础性规范，亦为判断ISP保护个人信息措施的必要性与可期待性之重要标准。只要违反了成文法强制性规定，或者未尽到成文法设定的义务，即构成违反安全保障

义务。如《网络安全法》第22条规定“网络产品、服务的提供者不得设置恶意程序；发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告”。该条内容即包含了义务性措施与强制性措施。如果ISP违反了该条规定，即可立即判定存在“过错”。

其次是行业标准或准则。如果缺乏明确的义务性强制性规范，还可以寻求诸如行业标准、行业自律性指南等行业同行准则作为判断必要性的依据。一方面是基于我国法律明文规定，如《网络安全法》第22条规定：“网络产品、服务应当符合相关国家标准的强制性要求”；另一方面，行业标准或准则是行业内自我约束、自我管理的基本标准，相当于该行业集体对社会的承诺。ISP作为网络社会的主导者和网络服务业的最主要参与者，其必定参与行业标准和指南的制定。因此，行业标准和指南的规定也相当于对他们自身的约束和规范。此种做法的实践意义是以行业准则作为义务内容，借以弥补成文法义务性强制性规范不足的缺失。目前我国在个人信息保护领域，有诸如《信息安全技术公共及商用服务信息系统个人信息保护指南》等。在比较法上，亦有一些典型判例，凡举一例：2015年，在美国第三巡回上诉法庭判决的Federal Trade Commission诉Wyndham Worldwide Corp.案之二审上诉案件(以下简称“Wyndham案”)中，[①]上诉人Wyndham环球公司及其附属公司在不同系统之间经由内部计算机网络实现数据的相互连通，存储了大量的用户个人信息。然而该系统网络于2008年至2009年期间遭受了黑客的3次攻击，导致大量个人信息流出，大量用户的信用卡信息被盗，造成巨额损失。Wyndham公司公布的隐私条款中宣称自己已遵守“行业标准操作”，[②]然而事实并非如此。联邦商务委员会列举了7项被告“不合理的网络安全操作”，包括在关键网络点未使用任何防火墙来限制物业管理系统与外部网络之间的连接，未对特定用户信息进行任何加密操作，未采取合理的应急事件响应程序等。该案审理中，法院在判断Wyndham的网络安全措施是否合理时亦参考了联邦商务委员会发行的相关“指南”。尽管“指南”中并没有明确到底何种程度可以被算作履行了合理公平的安全保障义务，但也明确地反对并列举了许多不合格的具体实践操作，包括：防火墙防御能力不够，未对存储于系统内的信息进行加密，未对无授权的外部通信请求加以限制，未在收到攻击后使用合理手段检测和预防网络再次遭到攻击等。上述经验说明，以相对完善的行业标准或行业自律规范作为判断“过错”的标准是一种可行的路径。[③]

再次，还应包括“一错再犯”情形。如果某一ISP曾因泄露个人信息被处罚，并要求对其安全系统加以整改。该提供商整改后又发生类似事件，则法院可以前一次的

① *FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. N.J. Aug. 24, 2015).

② *FTC v. Wyndham Worldwide Corp*., 10 F. Supp. 3d 602: “Consumers could not take steps to avoid Wyndham’s unreasonable data security [before providing their personal information] because Wyndham falsely told consumers that it followed ‘industry standard practices’.”

③ 中国互联网协会于2002年公布了《中国互联网行业自律公约》，倡议互联网全行业从业者加入本公约，并要求成员“自觉维护消费者的合法权益，保守用户信息秘密；不利用用户提供的信息从事任何与向用户作出的承诺无关的活动，不利用技术或其他优势侵犯消费者或用户的合法权益”。

处罚决定作为其此次认定“过错”的依据。又如某ISP曾经发生过个人信息大规模泄漏事件，但经媒体报道后，仍未认真整改，以致再次发生类似事件。此时，法院亦可认定为存在“过错”。此做法脱胎于行政法上的“首违免罚”制度。该制度对于一些违法程度不严重，危害不大的行为，行政执法中应贯彻“包容审慎监管”理念，对一些违法行为在首次被执法机关发现后，只要积极改正、补救，可以不予处罚。但是如果同一主体再次被发现同样的违法行为，则应予以处罚。该做法隐含了“可期待性”要件的认定标准，即同样的错误再犯，行为人的“过错”程度即达到了承担法律责任的程度。现代黑客技术高度发达，网络安全建设难以完全防范。有一些网络平台虽然加装了安全设施，如防火墙等，仍无法完全避免。此时如果仅以“信息泄露”之结果作为过错认定依据显然不公，但如果已经经历过一次“泄露”，又发生类似事件，则其“过错程度”即大幅度上升，此时应当认定ISP之“过错”。

最后是公共政策一般准则。一个地区的公共政策脱胎于时代的需求，又深刻融于地区法律体系之中。近20年来，我国电子商务行业蓬勃发展，产值大幅提升的背后也埋下了许多有关个人信息的隐患。这些隐患可能成为公民个人信息被不法侵犯的“入口”；另一方面，就ISP与用户之间的关系来看，应对前者加以控制。前者基于商业特性，往往需要收集大量的用户个人信息，相对于后者来说是占据了更强势地位的主体；若对前者的逐利性不加以控制，则有可能使后者的个人信息时常处于危险状况中。因此，在发展网络产业的同时，对个人信息进行保护已经是社会的共识，亦是一项公共政策的一般准则。对于一些网络平台泄露个人信息事件，可能一时找不到法律依据，亦找不到行业规范，但可以公共政策的一般准则作为确定过错的依据。

比较法上，欧盟各国对企业获取个人利益并获利，应当承担保护个人信息的义务这一点已然形成共识。美国法上，“公平实践信息的基本原则”第5点即明确，任何产生、保存、使用或传播可识别出个人身份的数据的机构必须确保数据对拟使用的目的是可靠的，并采取合理的措施预防数据的不当使用。在英国，以肯尼斯·杨格(Kenneth Younger)为首的隐私委员会于1972年发布的《关于个人数据自动处理的安全建议》(Specific Safeguards for Automated Personal Data Systems)中亦提出所谓的“安全性原则”：即系统使用者应预先说明系统应当达到的安全防护水平，采取适当措施避免信息被误用或滥用，并应当建立监测系统，防止各类违反安全的问题发生。但公共政策的一般准则较为原则和笼统，易被滥用，须在其他情形无法适用，但又依一般法理明显存在“过错”的情形下方可适用。

三、责任的落实：赔偿模式之选择

（一）现行侵权立法提供的模式

在网络服务提供者侵权的法律规制(含赔偿责任)方面，我国《侵权责任法》提供了两个路径：“连带责任+通知与删除规则”(下称“模式一”)和“相应的补充责任”(下称“模式二”)。

模式一主要规定于《侵权责任法》第36条，[①]其核心在于认为传统的网络侵权责任中，网络服务提供者多数情况下作为间接侵权人承担连带责任。这一观点源自网络著作权侵权，[②]后被《侵权责任法》所吸收并拓展至整个侵权领域。连带责任指被侵害人有权请求加害人中的任何一人或数人请求承担损害赔偿责任，任何加害人都有义务向被侵害人负全部赔偿责任。在连带责任中，多个加害人共同承担责任的原因在于其共同侵权行为的可受责难性。在网络用户利用网络服务实施侵权行为的情况下，网络服务提供者依法所承担的责任是根据间接责任规则，基于他人直接侵权行为所产生的责任。虽然网络服务提供者并不主动实施信息交换行为，仅处于消极中立地位提供网络搜索、网络接入等技术服务，但对于他人的直接侵权行为，ISP起到帮助侵权作用，因此与直接侵权人构成一个整体实施了共同侵权行为，在责任承担形式上不仅要对自身的间接侵权行为负责，也要对直接侵权人的行为负责，承担连带责任。

出于公共政策考量和利益平衡，美国1998年《数字千年版权法》在第512条设立了“通知与删除”规则，即“避风港规则”。该规则授权被侵权人向ISP发出通知，后者采取删除、屏蔽、断开链接等措施后可以免责,否则要对损害扩大部分承担连带责任。我国《侵权责任法》将主体范围扩大到了所有“网络用户，网络服务提供者”，形成了目前的规制模式。该模式要点在于：1.网络服务提供者仅对接到通知后拒绝采取措施导致的扩大损失与直接侵权人承担连带责任；2.网络服务提供者对接到通知之前的损害不负责。

模式二的法律依据主要来自《侵权责任法》第37条规定的“安全保障义务”条款。该条款要求特定的义务主体对进入其控制领域的人负有保障其安全的义务。如果违反该义务，该义务主体要承担赔偿责任。该条又分为两种情形：无直接侵权人和有直接侵权人。前一种情形则直接由安全保障义务人承担责任，后一种情形则先由直接侵权人承担，赔偿不足的部分再由安全保障义务人承担相应的补充责任。此处的“相应的补充责任”模式一般存在于三方主体关系下。其中第一方是直接加害人，第二方是受害人，第三方是负有安全保障义务的主体。

第三方“相应的补充责任”应有两层含义，即“相应”和“补充”。所谓“相应”，指的是与过错程度相对应，如果按照“原因力”理论，则应与“原因力”大小相对应。[③]而对于“补充”二字，则有两重含义。一是，第三方须在第一方现行承担责任后，对于其无力承担部分再行补充承担。此处存在某种极端情况，即第一方可以承担全部赔偿责任，此时第三方无需承担赔偿责任；二是，第三方承担的补充责任的大小一般不超过第一方的责任份额。对于此点，由于法律并无明文规定，需要在司法

① 《侵权责任法》(2009年12月26日通过)第36条：“网络用户、网络服务提供者利用网络侵害他人民事权益的，应当承担侵权责任。网络用户利用网络服务实施侵权行为的，被侵权人有权通知网络服务提供者采取删除、屏蔽、断开链接等必要措施。网络服务提供者接到通知后未及时采取必要措施的，对损害的扩大部分与该网络用户承担连带责任。网络服务提供者知道网络用户利用其网络服务侵害他人民事权益，未采取必要措施的，与该网络用户承担连带责任。”

② 吴汉东. 论网络服务提供者的著作权侵权责任[J]. 中国法学, 2011(2): 38–47.

③ 张新宝. 侵权责任编起草的主要问题探讨[J]. 中国法律评论, 2019(1): 133–144.

中综合加以认定。[①]还有一种特殊情形，即没有第三方采取入侵，窃取等方式获得ISP所存储的个人信息，完全由于ISP自身失误，导致个人信息外泄，并流向不特定主体。此时，ISP应承担全部赔偿责任。对此，欧盟《通用数据保护条例》(GDPR)第82条亦明文规定：1.任何因为违反本条例而受到物质或非物质性伤害的人都有权从控制者或数据者那里获得对损害的赔偿。2.任何涉及到处理的控制者都应当对因为违反本条例的处理而受到的损害承担责任。对于处理者，当其没有遵守本条例明确规定的对处理者的要求，或者当其违反控制者的合法指示时，其应当对处理所造成的损失负责。

（二）对二种模式的评述与选择

模式一所依据的是《侵权责任法》中用以规范和调整网络侵权的最重要条款，似乎应被优先考虑为责任承担的法律依据，但此结论未必正确。理由如下：该模式旨在限制和惩罚ISP的帮助侵权行为，以连带责任对帮助侵权进行惩罚和规制，同时亦兼顾互联网行业之发展与勃兴。然而ISP违反对个人信息的安全保障义务与ISP的帮助侵权存在着本质的不同，ISP不构成对个人信息的帮助侵权。

所谓帮助侵权的构成要件有三：(1)存在直接侵权行为；(2)间接责任人认识到直接侵权行为的存在；(3)帮助直接侵权人实施了侵权行为。[②]ISP违反安全保障义务时不满足第二和第三个构成要件。前述Wyndham案中，黑客前后共对Wyndham集团旗下酒店的个人信息系统进行了3次安全攻击，但直到第三次攻击发生后该集团才对本案中的直接侵权行为有所察觉。Wyndham集团未采取有效措施防止黑客攻击，亦承担赔偿责任，但整个过程中其并未主动实施帮助黑客侵权的行为。

质言之，在其他类型网络侵权案件中，侵权人借助网络平台实施侵权行为，一方面存在“借助”因素，在接到受害人通知后拒绝删除还意味着“明知”；另一方面，发布侵权信息行为亦会给ISP带来流量、点击率等益处。而在ISP违反对个人信息安全保障义务的案件中，不存在ISP主观上知道(或推定知道)有第三人侵犯其存储的个人信息的因素，亦不存在任何“帮助”。因此，ISP违反安全保障义务无法与直接侵权行为人的行为构成共同侵权和连带责任，亦不应适用模式一。

模式二是我国《侵权责任法》对于不作为侵权的立法方式。虽然其不针对网络侵权，但其对于本文所论述的ISP对个人信息的安全保障义务却可能更有借鉴意义与价值，主要理由：(1)二者调整对象属于同一类型，都是消极的不作为侵权。即出于某些特定目的或保障某些特定的法益(权利)，法律对某些主体课以特定的保护(作为)义务，如果履行该义务就将承担赔偿责任。无论是《侵权责任法》的场所安全保障义务还是本文所讨论的网络空间安全保障义务，均属上述类型，只不过前者发生在现实社会，而后者发生在网络空间。违反这些义务均构成不作为侵权。(2)二者规制方式高

① 对此，张新宝教授认为“补充”的含义应解释为不超过50%。参见：张新宝. 我国侵权责任法中的补充责任[J]. 法学杂志, 2010(6): 1–5.

② 吴汉东. 论网络服务提供者的著作权侵权责任[J]. 中国法学, 2011(2): 38–47.

度相似。从规制方式看，二者均通过法律设定特定的作为义务。该义务以保障特定法益(权利)的安全为目的，以“注意义务”为核心，以义务人的相应补充赔偿责任为法益受到损害的救济手段。“保障义务”是“注意义务”的特殊形式。(3)更有利于受害人与安全保障义务人之间的利益平衡。补充责任制度使受害人得到了直接侵权人以及补充责任人的双重赔偿保障，但其求偿选择权又被限制；同时补充责任人不仅在赔偿责任上排位于直接责任人之后，仅需承担直接责任人赔偿不足部分，从而大大减轻负担。双方由此实现了利益的基本均衡。

结 论

在ISP对个人信息应负安全保障义务的前提下，如果其未能适当履行该义务，致使其保有的个人信息泄漏，应当按照“相应的补充责任”模式承担侵权责任后果。即在无第三人入侵的情况下，应由ISP依照其过错程度承担相应责任；在有第三人入侵的情况下，应先由第三人承担赔偿责任，如果第三人赔偿不足的，再由法院根据ISP的过错程度，判令其承担相应的补充责任。

回到本文引论部分所提出的案件，原告个人信息在被告运营的订票网站泄漏，但该案应有其他直接侵权人。故如果找到该直接侵权人，法院应要求原告增列直接侵权人为被告，再按“相应的补充责任”模式，予以判决。如果找不到直接侵权人，亦不应赔偿全部责任，而应按照“相应的补充责任”模式，在不超过50%的范围内判决承担。

【作者简介】李 磊： 上海对外经贸大学法学院副教授，硕士生导师，法学博士。研究方向：民商法。

On Tort Remedy of Personal Data Leakage by ISP

LI Lei

(School of Law, Shanghai University of Business and Economics, Shanghai 201620, China)

Abstract: Article 111 of China’s“Civil Law”, which presents a new legislative approach to personal information protection, requires that acquirer and keeper of the personal information, such as Internet Service Provider (ISP), should bear the duty of security protection. The duty above includes two parts: general duty and period duty. And the context of the duties can be found in other related laws and regulations. It’s difficult to find the faults and reasons. Theoretically, the breach of the duty of security protection leads to fault. In terms of way of accountability, determination of fault should be made by statutes, guidelines, and so on. There are two types of responsibilities in the Chinese civil law. One is notification-delete model, the other is supplementary model. And supplementary responsibility should be adopted in these cases.

Keywords: duty of security protection; internet service provider; personal data protection

（责任编辑：黄志瑾）