昆明学院学报　2018，40（2）：49～54　ISSN 1674－5639　CN 53－1211/G4
Journal of Kunming University　【法学】

个人信息刑法保护面临的困境与出路

吴海波
（安徽大学 法学院，安徽 合肥 230601）

摘要：在大数据信息时代的今天，侵犯公民个人信息的犯罪日益猖獗。《中华人民共和国刑法》经过数次修正，将侵犯个人信息罪写入法律。但在实践中，法律解释的局限性和高科技犯罪取证困难等，使得个人信息的保护仍面临着各种现实困境。从完善我国现有的立法系统出发，出台专门的《个人信息保护法》，加强网络安全管理，提升民众安全防范意识，才能正确有效地遏制信息外泄，保护公民权益。

关键词：公民；个人信息；信息犯罪；刑法保护
中图分类号：D924.3　**文献标识码**：A　**文章编号**：1674－5639（2018）02－0049－06
DOI：10.14091/j.cnki.kmxyxb.2018.02.008

Dilemma and Measures about Criminal Law Protection of Personal Information

WU Haibo
（Faculty of Law，Anhui University，Hefei，Anhui，China　230601）

Abstract：In the era of large data and information，the crime of infringement of personal information of citizens is becoming more and more rampant. The criminal law of the People's Republic of China has been amended several times to put the crime of personal information into the law. However，in practice，the limitations of legal interpretation and the difficulty of obtaining evidence from high－tech crimes still give the protection of personal information the various practical difficulties. With improving Chinese existing legislative system，the specific law should be published to protect personal information，and network security management should be strengthened and public awareness of safety and security should be enhanced so as to effectively curb information leakage and protect citizens' rights and interests.

Key words：citizen；personal information；information crime；criminal law protection

随着大数据时代的来临，信息技术给人们带来便捷服务的同时，也产生了相应的负面效应。所谓“大数据”，就是信息爆炸时代产生的海量数据，其中就包括了公民的个人信息。不法分子往往利用网络等高科技手段，骗取公民个人信息，谋取非法利益，给民众带来损失的同时也造成了严重的社会影响。因此，公民个人信息的安全理应得到重视；针对信息犯罪的频繁发生，完善相关的刑事法律，发挥刑法规制作用，刻不容缓。

一、历来刑法对侵犯个人信息犯罪的规制

为适应信息时代的需要，遏制侵犯个人信息犯罪日益增长的势头，我国在《中华人民共和国刑法修正案（以下简称《刑法修正案》）（七）》中，增加了出售、非法提供公民个人信息罪和非法获取公民个人信息罪。[①]这两个罪名的增设，体现了国家对公民个人信息的保护已经重视，开始采用刑法加以

收稿日期：2017－09－09

作者简介：吴海波（1994—），男，安徽合肥人，硕士研究生，主要从事刑法研究。

①《中华人民共和国刑法修正案（七）》第7条规定：国家机关或者金融、电信、交通、教育、医疗等单位的工作人员，违反国家规定，将本单位在履行职责或者提供服务过程中获得的公民个人信息，出售或者非法提供给他人，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；窃取或者以其他方法非法获取上述信息，情节严重的，依照前款的规定处罚。

规制，具有里程碑式的意义。但是，这两个罪名中对相关概念并没有做出明确的解释说明，比如什么是“公民个人信息”？哪些行为属于“情节严重”的范畴？经过实践的检验发现，该条款在司法适用中会出现分歧和争议。例如，2015 年 6 月发生的王某甲案，[1]公安机关以被告涉嫌非法侵入计算机信息系统罪为由，对其逮捕归案，但法院最后却以侵犯公民个人信息罪定罪判刑。罪名适用上出现冲突，正是法律规定不成熟和适用范围不明确的表现。

继《刑法修正案（七）》后，《刑法修正案（九）》对这两个罪名重新进行整合，将“出售、非法提供公民个人信息罪”和“非法获取公民个人信息罪”整合为“侵犯公民个人信息罪”，并做了实质性的修改。① 首先，去掉了特定单位工作人员的限制，将犯罪的主体从特殊主体扩大到一般主体；其次，将“上述信息”强调为“公民个人信息”，行为方式强调“提供”而不是“非法提供”，在表述上更为具体、严谨；最后，提高了有期徒刑的刑期，罚金刑从选择并处或单处也转变为并处，反映了国家对侵犯公民个人信息犯罪惩处力度的加大。但是，《刑法修正案（九）》对公民个人信息的概念仍未具体明确，定罪量刑的标准也并不清晰，司法实践中的争议仍然存在，亟需通过司法解释予以明确。

二、刑法规制的新态势

鉴于上述问题未得到有力解决，加之电信诈骗的猖獗，使得侵犯公民个人信息犯罪处于高发态势，社会危害性日益突出。因此，最高人民检察院和最高人民法院于 2017 年 5 月 8 日公布了《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》（以下简称两高《解释》），自 6 月 1 日起施行。作为最新的司法解释，其主要解决了如下问题：

（一）公民个人信息范围的确定

这是长久以来刑法都未具体规定的问题，在两高《解释》中，第一条就对此概念加以认定：“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。”该定义与美国《隐私法案》对公民个人信息范围的定义模式有异曲同工之妙。美国《隐私法案》确定公民个人信息的概念采用的是概括列举混合模式，这种模式将抽象概括与逐一列举相结合，在法条上表述为：“个人信息包含与公民个人相关的单项信息或者组合信息，包括但不限于教育、医疗、金融等领域的相关信息以及类似姓名、身份证号等用以识别特定主体的身份标记，如指纹、声纹或照片等。”这种定义模式将概括型定义模式和列举型定义模式的优势相结合，并弥补了两者的缺陷，能够较好地确保对公民个人信息范围界定的延展性，从而成为了各国普遍认可的定义模式。[2]

回看我国两高《解释》对公民个人信息的定义，首先，以概括的方式，将个人信息的基本范围界定在“识别特定自然人身份”或“反映特定自然人活动情况”这两个特征上，满足二者其中之一就属于公民个人信息。之后，又以列举的方式，对公民个人信息进行同类解释，在两个特征的基础上，具体明确了哪些信息属于公民个人信息。最后，以“等”字加以兜底，体现解释的严谨性。该定义综合了我国学界对公民个人信息的各类观点，如《中华人民共和国个人信息保护法示范法草案学者建议稿》认为的个人信息应当具有识别性；[3]再比如，参考英美等国，以隐私权理论作为个人信息保护的基础，将个人信息和个人隐私等同看待。总之，两高《解释》对公民个人信息的定义进行了理论经验的总结，是在长期的理论基础积累下的、历史与现实相统一的、较为科学合理的规定。其使我国刑法中个人信息的范围明朗起来，有利于实践中正确的定罪和量刑。

---

①《中华人民共和国刑法修正案（九）》第 17 条规定：违反国家有关规定，向他人出售或者提供公民个人信息，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。违反国家有关规定，将在履行职责或者提供服务过程中获得的公民个人信息，出售或者提供给他人的，依照前款的规定从重处罚。窃取或者以其他方法非法获取公民个人信息的，依照第一款的规定处罚。

（二）本罪“情节严重”标准的明确

《刑法修正案（九）》中，将情节严重作为侵犯公民个人信息犯罪的入罪标准。但何谓“情节严重”，却并没有明确的衡量标准。这会导致司法实践中法官难以把握，罪与非罪、罪轻与罪重，全都由法官自由裁量和判断，难免造成判决不公的现象。对此，两高《解释》中运用了大量篇幅，对侵犯公民个人信息犯罪的定罪量刑标准进行了规定，以弥补之前的《刑法修正案》在这方面规定的缺失。

《解释》出台前，学界关于情节严重标准，就有若干不同的观点，大体分为三要件说和四要件说两类。[4]三要件说主张认定“情节严重”，要考虑三方面内容，包括行为的目的、行为造成的结果和行为的客观表现。这三个条件并不是要同时满足，但有考虑上的先后顺序。具体而言，为了实施违法犯罪活动而侵犯公民个人信息是首要考察因素；其次，考虑是否造成严重后果，如干扰到公民个人的正常生活或带来了较大的经济损失；最后，若无法确定前两个条件，那么可以考虑到第三个要件，即采取的手段是否恶劣、获得的个人信息数量是否较多、窃取或提供个人信息的次数是否频繁等行为的客观方面，作为认定情节严重的标准。四要件说仅在三要件说的基础上，增加了造成国家或社会重大利益损失的结果要件。无论是三要件说还是四要件说，二者的内涵是一致的，都是从侵害行为的性质出发，以行为性质认定情节严重标准的同时，也不排除考虑行为结果的影响。

立足现有的学术观点，结合实践经验，两高《解释》对“情节严重”进行了具体而细致的规定。[①] 这些规定中，有根据行为目的规定的情节，如第二项；有基于数量标准规定的情节，如第三、四、五项；更有不拘泥于理论观点，较为新颖的规定，如第九项：曾因侵犯公民个人信息受过刑事处罚或者二年内受过行政处罚，又非法获取、出售或者提供公民个人信息的，属情节严重。这里借鉴了刑法上累犯从重处罚的理念，虽然不是累犯，但存在前科，社会危害性较大，归为情节严重是理所应当。此外，两高《解释》还补充规定了“情节特别严重”的情节，包括：造成被害人死亡、重伤、精神失常或者被绑架等严重后果的；造成重大经济损失或者恶劣社会影响的；数量或者数额达到前款第三项至第八项规定标准十倍以上的及其他情节特别严重的情形。可以说，本次解释对侵犯个人信息犯罪的“情节严重”规定达到了多角度、宽范围的覆盖。是否有成效，就要在日后的司法实践中加以检验。

（三）本罪涉及刑事政策、单位犯罪、数额计算等问题的解决

法律解释的合理性原则，要求法律解释必须以党的政策和国家政策为指导。因为与法律相比，政策更具有灵活性和针对性，更能够及时反映社会发展的需要。[5]两高《解释》响应我国宽严相济的刑事政策，在规定了罪重的一系列条款的同时，对侵害个人信息犯罪的从宽处理也有所涉及。如第十条规定：“实施侵犯公民个人信息犯罪，不属于情节特别严重，行为人系初犯，全部退赃，并确有悔罪表现的，可以认定为情节轻微，不起诉或者免予刑事处罚。确有必要判处刑罚的，应当从宽处罚。”体现了刑法的谦抑性。这不仅坚持了法律解释的合理性原则，也是法治内在的特点和要求。

①《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》第五条规定：非法获取、出售或者提供公民个人信息，具有下列情形之一的，应当认定为刑法第二百五十三条之一规定的“情节严重”：（一）出售或者提供行踪轨迹信息，被他人用于犯罪的；（二）知道或者应当知道他人利用公民个人信息实施犯罪，向其出售或者提供的；（三）非法获取、出售或者提供行踪轨迹信息、通信内容、征信信息、财产信息五十条以上的；（四）非法获取、出售或者提供住宿信息、通信记录、健康生理信息、交易信息等其他可能影响人身、财产安全的公民个人信息五百条以上的；（五）非法获取、出售或者提供第三项、第四项规定以外的公民个人信息五千条以上的；（六）数量未达到第三项至第五项规定标准，但是按相应比例合计达到有关数量标准的；（七）违法所得五千元以上的；（八）将在履行职责或者提供服务过程中获得的公民个人信息出售或者提供给他人，数量或者数额达到第三项至第七项规定标准一半以上的；（九）曾因侵犯公民个人信息受过刑事处罚或者二年内受过行政处罚，又非法获取、出售或者提供公民个人信息的；（十）其他情节严重的情形。

对于单位侵犯个人信息的，为了填补立法的空白，本解释也在相应条款中加以明确。[①] 在数额计算方面，明确了如何计算侵犯公民个人信息的条数问题，对非法获取公民个人信息后又出售或者提供的，公民个人信息的条数不重复计算；向不同单位或者个人分别出售、提供同一公民个人信息的，公民个人信息的条数累计计算；对罚金刑的数额也依法划分了范围，一般在违法所得的一倍以上五倍以下。这些规定，为日后侵犯个人信息犯罪的定罪和量刑提供了法律依据。

两高《解释》的发布，证明了我国刑事法律在保护公民个人信息的道路上，正积极应对时代的变化，响应社会民众的需求，是法制进步的体现。但是，由于法律解释的局限性和现实情况的复杂性，关于侵犯个人信息犯罪的刑法规制和公民个人信息的刑法保护，仍面临较多的困境。

三、应对侵犯个人信息犯罪的困境

（一）信息犯罪本身的复杂性

随着网络技术和计算机技术的飞速发展，科技的“双刃剑”特性逐渐显现。在侵犯公民个人信息的犯罪中，犯罪分子往往利用高科技手段，以电脑、手机为载体，进行公民个人信息的获取，以谋取不法利益。这种情况下，实施信息犯罪的人往往具有较强的计算机知识背景和娴熟的计算机操作技能。他们利用信息系统的漏洞，借助四通八达的网络，对各种电子数据、客户资料等信息进行窃取和利用，体现了犯罪手段的智能性。同时，信息犯罪的地点往往不受时间、地域的限制，可以通过网络跨地域远程进行信息窃取，其罪恶的源头更可能来自全球的任何一个终端，具有极强的不确定性。如“3·10”特大跨境电信诈骗案，是典型的侵犯并利用公民个人信息进行诈骗活动的案例。其中，就涉及了柬埔寨、印尼等国和地区的电信诈骗犯罪集团，涉案范围之广，可以称之为公安机关目前侦破的最大规模的电信诈骗犯罪案件。而利用电子设备窃取并利用公民个人信息进行非法活动，往往是瞬时发生的，不会对硬件造成任何损坏，大多数的犯罪证据也都可以从系统中删除、销毁，因此很难侦破犯罪人的行踪，对犯罪的取证也造成严重困难，具有极强的隐蔽性。这些犯罪自身的复杂特点，决定了现阶段很难从技术上发现行之有效的手段，彻底解决个人信息的泄露而遏制信息犯罪。

（二）立法面临的瓶颈

尽管本次的两高《解释》对侵犯公民个人信息犯罪的部分问题加以补充和完善，但是，依旧存在考虑问题不够全面、处理方式不够到位之处，作为立法上的瓶颈，有待突破的几点如下：

1. 外籍人和无国籍人个人信息的保护问题

作为侵犯个人信息犯罪的被害人，公民在本罪中的地位是举足轻重的，确定被侵犯人是否为公民，是定罪的要件之一。但是，我国刑法并未在此罪名中明确规定公民的范畴，因此只能以我国宪法上对公民的规定作为标准，即具有中华人民共和国国籍的人，都是我国公民。那么，司法实践中就会面临一个问题，当我国境内的无国籍人士或者外籍人士的个人信息受到侵犯，该适用哪条法律去规制？若是依然以侵犯公民个人信息罪名去定罪，显然是不恰当的，因为犯罪的被害人不符合我国宪法对公民的界定。那么，无国籍人士或者外籍人士的个人信息如何获得有力的刑法保障，这是个立法上的缺失。

2. 已故公民个人信息的保护问题

对于这个问题，我国学者们也有很大的争议，主要存在两种观点。其一，持积极态度，认为我国公民虽然已经过世，理论上丧失了自然人的主体资格，但其个人信息却并没有随之消失，其中仍有很多有价值的信息，可被犯罪人利用来对死者的亲友或他人进行不法活动，因此已故公民的个人信息有必要受到刑法保护。其二，则持相反观点，认为既然已故公民已经丧失自然人的主体资格，而我国宪法规定的公民必须为自然人，那么，死者的个人信

①《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》第七条规定：单位犯刑法第二百五十三条之一规定之罪的，依照本解释规定的相应自然人犯罪的定罪量刑标准，对直接负责的主管人员和其他直接责任人员定罪处罚，并对单位判处罚金。

息就不属于公民个人信息，因此也就无法受到刑法保护。

笔者赞同第一种观点，因为其与立法的初衷是相一致的。刑法设立本罪的目的就是肯定公民个人信息的价值以及预防个人信息被侵犯所导致的严重后果，而被侵犯公民是否在世这个问题似乎并不是那么重要。毕竟，很多公民的个人信息并不会因本人的离世而消失，其价值还是客观存在的。如果过于教条地割裂已故公民个人信息与公民个人信息的关系，实践中若出现利用死者个人信息犯罪的情况，可能会产生法律适用上的难题。

（三）其他现实困境

除了信息犯罪本身的复杂性以及立法上的缺陷以外，还存在如信息行业的不正当竞争泛滥，在各种利益的驱动下，银行、保险公司、通讯企业等泄露客户信息的行为时有发生，公众自我保护意识的缺乏等，都或多或少为信息犯罪打开方便之门，对我国刑法保障公民个人信息安全、维护信息安全畅通等，提出了严峻的挑战。采取相应措施保护公民个人信息安全，迫在眉睫。

四、保护个人信息的出路探索

（一）立法上的完善

侵犯公民个人信息犯罪的立法存在瓶颈，就要从立法上探寻突破该瓶颈的出路，可从以下几方面进行完善：

1. 特殊对象的个人信息保护

受公民这一条件的限制，无国籍或外籍人士的个人信息的保护这一块存在立法的空白。若单独增加一条侵犯外籍或无国籍人士个人信息罪，未免使得法律条文过于累赘。而如果对“公民”这一概念作扩大解释，使其包含无国籍人士和外籍人士，就与宪法中的公民概念相悖，有损立法的严谨性。因此，笔者认为可将“侵犯公民信息罪”改为“侵犯个人信息罪”，这实质上是将保护的对象扩大，从原先我国公民的个人信息扩大为我国境内所有人的个人信息，目的在于更全面的规制信息犯罪。

对于已故公民个人信息保护问题，必须在司法解释中予以明确，认定其具有保护的价值，侵犯已故公民个人信息或是利用其个人信息进行不法活动，都应认定为侵犯公民个人信息犯罪，追究其刑事责任。

2. 犯罪主体的区分量刑

众所周知，很多特殊的工作单位与公民的个人信息联系密切，如电信行业、银行、保险公司等。因此，特殊单位的工作人员能够轻易地接触到大量的公民个人信息，他们肩负着保护公民个人信息不被泄露的重要职责，若是其中存在利用职务之便非法窃取、出售、提供公民个人信息的现象，社会危害程度可见一斑。因此，笔者认为本罪的犯罪主体应当在量刑时有所考量。可在法条中补充从重处罚情节，若犯罪人是国家机关工作人员或从事与公民个人信息密切相关的工作之人员，利用职务之便，窃取公民个人信息进行非法活动，或将信息出售、提供给他人进行非法活动，理应从重处罚。

3. 尽快出台《个人信息保护法》

对于个人信息的保护，我国内地尚无此类专门性法律，而是散见于刑法、民法、行政法等多个部门法中，较为零散，不成体系。有学者指出具体数据：“当前我国关于公民个人信息保护的条文散落在 24 个相关法律文件中，其中属于国家法律的 3 部，属于行政法规的 1 部，属于司法解释的 2 部，其余的 18 部均为行政规章。”[6] 这种散落在一些法律条款中的信息保护规定已无法适应保护公民的尊严与权利的要求。[7] 因此，制定和颁布一部专门保护个人信息的法律刻不容缓，否则面对日趋严重的侵犯个人信息犯罪，公民的个人信息得不到保护的同时，社会的稳定也岌岌可危。

（二）从网络安全出发

网络是侵犯公民个人信息的重要渠道之一，鉴于此手段的隐蔽性与复杂性，除了完善立法，还应当从计算机技术、网络安全管理等方面进行综合防治。

1. 加强网络安全技术防范

“技术进步所带来的挑战，最终必须由技术本身来解决。”[8] 因此，治理利用高科技侵犯个人信息的犯罪，要特别注重技术防范。目前的技术性防

范措施主要有设置防火墙、安装杀毒软件、对重要文件进行加密处理等，较为浅显和单一。应进一步构筑安全的计算机信息系统，加强网络监管手段的多样性，使网络防御技术尽可能将犯罪分子拒之门外。在技术上填补网络安全漏洞，就是从源头堵塞了犯罪的重要途径，不失为遏制信息犯罪行之有效的手段。

2. 提高民众网络安全意识

树立安全观念，提高公民网络安全意识，是遏制个人信息犯罪的必要环节。长期的重视应用、轻视安全，导致计算机应用技术发展很快，而安全防范技术明显滞后。[9]在很多信息犯罪中，往往是犯罪分子在作案前并没有固定的目标，只是用工具对互联网上的机器随机扫描，发现存在安全系统漏洞的用户，犯罪分子就会趁机而入，对用户的个人信息大肆收集和窃取，导致公民个人信息的泄露。因此，我国应在普及计算机技术的同时，开展网络安全的宣传教育，推动网络安全技术，使广大用户时时提高警惕，自觉利用防火墙或加密的手段，对个人信息做好安全防范工作。

3. 网络伦理的构建

网络上侵犯个人信息的犯罪严重化，与互联网带来的道德失控密切相关。有学者认为："展望未来，要通过技术或常规立法程序去遏制信息犯罪活动困难重重，最根本的解决办法只有一条，那就是道德与人生价值观。要让人们有这样的信念：偷窃、解密和私自侵入是不可取的。"[10]因此，在全社会树立科学的网络是非荣辱观，使民众达成一致的认识，即在网络上对个人信息的窃取和破坏，应当受到网络伦理的谴责和刑法的追究，才是有效制止侵犯个人信息犯罪的根本之道。当然，这种理想化的理念，只能在未来有所期待，现实有效的遏制犯罪行为，还是要通过网络安全技术的进步和相关法律法规的完善。

但是，刑法的使命并非以设定严苛的刑罚和条条框框的规定来阻碍信息化的发展，法律都应顺应时代的潮流而非逆流而上。作为惩罚犯罪和保障人权相统一的刑法，真正的作用是通过合理的刑事立法来遏制公民个人信息泄露的现象，规制侵犯个人信息的犯罪，将信息时代的弊端带来的危害降到最低，以期在信息的自由流通与公民个人信息安全的保护之间寻求充分的平衡。要达到这样的效果，我国的刑事法律还任重道远。

［参考文献］

［1］山东省平邑县人民法院. 王某甲侵犯公民个人信息一审刑事判决书［EB/OL］.［2017 - 03 - 29］. http://wenshu.court.gov.cn/content/content? DocID = c2a5eb33 - 9241 - 4122 - 86db - a728017d1374&KeyWord.

［2］范雅璐. 出售、非法提供公民个人信息罪若干疑难问题探讨［D］. 上海：华东政法大学，2015.

［3］齐爱民. 中华人民共和国个人信息保护法示范法草案学者建议稿［J］. 河北法学，2005（6）：2 - 3.

［4］柴梦迪. 我国公民个人信息的刑法保护研究［D］. 海口：海南大学，2016.

［5］张文显. 法理学［M］. 北京：北京大学出版社，2012：238 - 239.

［6］卢建平. 我国侵犯公民个人信息犯罪的治理［J］. 法律适用，2013（4）：58 - 60.

［7］候一平. 呼吁尽快出台"个人信息保护法"［J］. 中国人大，2016（19）：48 - 59.

［8］CLARK C. The answer to the machine is in the machine［J］. In the Future of Copyright in a Digital Environment，1996（10）：139 - 141.

［9］康树华，张小虎. 犯罪学［M］. 北京：北京大学出版社，2015：392 - 393.

［10］黄群庆. 信息空间的犯罪活动［J］. 世界科学，1996（8）：36 - 37.