公民个人信息保护研究——基于电信网络诈骗犯罪视角

杨 旭，温小惠

贵州民族大学法学院 贵州贵阳

【摘要】数据信息时代之下，电信网络诈骗犯罪频发，最重要的原因之一便是由于当前个人信息泄露严重，为犯罪分子实施犯罪行为提供先决条件。导致电信网络诈骗犯罪与个人信息泄露两者之间的“产生”和“繁荣”互为因果，一方面个人信息的产生和发展，在数据算法机制的运算下，成为电信诈骗犯罪的必备要素；另一方面，电信网络诈骗犯罪的高效非法回报驱使非法组织和个人继续使用贩卖、爬取、盗取等非法手段获取个人信息，侵犯公民的人身、财产权益。从三个层面对个人信息的保护予以分析：一是在信息处理上，积极履行数据安全保护义务和合法处理个人信息的原则；二是在司法实践中，建立打击网络诈骗犯罪的合作联动机制，以期保护公民的人身和财产权益；最后是对出境数据信息的规制上进行探讨，以期个人信息主体对其个人信息获得合法有效救济。

【关键词】电信网络诈骗犯罪；公民个人信息；个人信息保护；数据信息

【基金项目】2021 年度贵州民族大学法学院法律专业学位硕士生工作站（检察方向）校级课题《公民个人信息保护研究--基于电信网络诈骗犯罪视角》（项目编号：20212JYB003）

Research on Citizens' Personal Information Protection ——Based on the Perspective of Telecom Network Fraud Crime

Xu Yang, Xiaohui Wen

Guizhou Minzu University, Huaxi Guiyang, China

【**Abstract**】In the era of data and information, telecommunication and network fraud crimes occur frequently. One of the most important reasons is that due to the current serious leakage of personal information, it provides a prerequisite for criminals to commit crimes. The "generation" and "prosperity" between the crime of telecommunication and network fraud and the leakage of personal information are mutually causal. On the one hand, the generation and development of personal information, under the operation of the data algorithm mechanism, has become an essential element of telecommunication fraud crimes; Obtaining personal information by illegal means such as theft infringes upon the personal and property rights and interests of citizens. The protection of personal information is analyzed from three levels. First, in information processing, actively fulfill the obligation of data security protection and the principle of legal processing of personal information; Second, in judicial practice, establish a cooperation and linkage mechanism to combat cyber fraud crimes, in order to protect citizens' personal and property rights and interests; finally, the regulation of outbound data information is discussed, in order to obtain legal and effective relief for personal information subjects for their personal information.

【**Keywords**】Telecommunication Network Fraud Crime; Citizens' Personal Information; Personal Information Protection; Data Information

随着数据信息时代的高速发展和《个人信息保护法》实施的背景之下，公众越发关注在当前的数据信息时代之下，应如何保护个人信息。一方面是因为当前侵犯公民个人信息的案件层出不穷，引发公众对犯罪的反思；另一方面是公众对个人信息保护的法律意识的增强。数据信息时代，公民个人信

作者简介：杨旭（1998-），男，贵州民族大学法学院，硕士研究生；温小惠（1986-），女，贵州民族大学法学院，硕士研究生。

息总是在未经过信息主体的许可即被收集、处理；此外是，公民的个人信息被人们无法知悉的方式应用于商业、教育、医疗等领域，甚至被用于非法领域。如电信网络诈骗、抢劫以及绑架等诸多危害人身、财产安全的犯罪行为之中。截至 2021 年年底，据工信部的数据显示，我国当前的移动用户数量规模已经高达 16.43 亿户。移动用户的迅速增长，为犯罪分子实施网络诈骗犯罪活动提供便捷条件。自 2021 年 4 月至 2022 年 4 月，全国公安机关深入开展整治电信网络诈骗违法犯罪“云剑—2021”等专项行动，针对电信网络诈骗犯罪先后组织开展全国集群战役 150 次，共破案 39.4 万件起，抓获犯罪嫌疑人 63.4 万名，破案件数比例上升 28.5%、抓获犯罪嫌疑人比例上升 76.6%，创历史新高[1]。

1 电信网络诈骗犯罪与公民个人信息保护之间的关系

《个人信息保护法》的出台，意味着我国当前的个人信息保护立法体系已然完善，但个人信息常以数据的形式在网络中传播[1]。个人信息的收集、处理、使用等行为方式的监管与当前的执法体系尚未跟进立法的步伐，呈现出不同步性，时常暴露出许多弊端。如，电信网络诈骗犯罪通过预先获取个人的信息，然后对相关个人信息进行分析处理，之后对信息所反应的主体实施精准诈骗行为，个人信息已然成为电信网络诈骗犯罪的先决条件[2]。基于此结论，必须对电信网络诈骗犯罪活动与个人信息的关系进行界定，使得公安机关在执法过程中能够精准打击诈骗行为，使得从源头治理这一治理模式取得成效。

1.1 电信网络诈骗犯罪概述

电信网络诈骗犯罪，是指犯罪分子通过非接触的方式，利用通讯网络工具和技术手段远程实施诈骗行为，非法获取被害人财产的统称[3]。并非刑法所规定的分则罪名之一，目前将其纳入到诈骗罪的范围之内，当然目前有学者倡导新设“电信网络诈骗犯罪”来概括此行为，但我国目前的立法体系已经趋向完善，且将电信网络诈骗犯罪行为纳入诈骗罪之中并无不妥之处，只需要在执法和司法的过程之中进行完善即可。在近几年，为该犯罪行为提供技术、通讯、洗钱等帮助服务行为不断增长，并逐渐呈现出产业化的形式，帮助信息网络犯罪活动罪已然成为与诈骗罪并发率最高的犯罪。

电信网络诈骗的起源，最早产生于我国台湾地区，犯罪嫌疑人基于被害人贪财的侥幸心理，实施诈骗行为，使被害人基于错误认识处分财物。而诈骗的方式从最早的虚假中奖方式到当前案发较多的刷单返利、杀猪盘以及网络贷款诈骗等方式，其诈骗的方式随着数据信息的发展不断复杂化，对打击犯罪行为造成严重的阻碍。特别是在疫情期间，衍生出一些不法分子假借“疫情行程流调、疫苗接种以及核算检测”等防疫之名，通过木马信息验证获取用户个人信息，让公众难以识别真假。“两高一部”针对电信网络诈骗犯罪，先后多次印发指导意见和办案指引[2]，指导相关机关打击处理电信网络诈骗犯罪行为。

1.2 公民个人信息保护概述

个人信息是指以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。[3]当前的数据信息时代之下，既要秉持充分利用个人信息促进各行各业发展，又要对个人信息的收集、处理中违反信息主体意愿、违反法律法规的行为进行强有力的法律规制。比如在公众的生活之中，某平台利用公民个人信息进行“大数据杀熟”，使某些用户在不知不觉中就花费更高昂的消费成本购买相关服务。从另一方面解释，由于大数据使得公民个人信息的价值提升，而非法收集、处理公民个人信息的风险降低，使得公民个人信息被大量非法处理，危害公民的人身、财产法益。比如 2016 年的徐玉玉案，一位 18 岁的花季少女在陷入电信网络诈骗中后，损失近万元的财物之后，因过于悲伤而失去生命。

1.3 电信网络诈骗犯罪与公民个人信息保护之间的关系

电信网络诈骗犯罪与个人信息泄露两者之间的“产生”和“繁荣”互为因果，一方面个人信息的产生和发展，在数据算法机制的运算下，成为电信诈骗犯罪的必备要素；另一方面，电信网络诈骗犯罪的高效非法回报驱使非法组织和个人继续使用贩卖、爬取、盗取等非法手段获取个人信息，侵犯公民的人身、财产权益。电信网络诈骗犯罪分子就是通过信息处理工具对被害人的个人信息全方位收集，经过算法机制进行智能分析，对所有信息用户

的基础数据进行分析，绘制出个人用户的数字模型图，然后通过专业的话术，对被害人实施诈骗。

（1）以数据信息为先决条件

电信网络诈骗犯罪的上游环节主要体现在其准备阶段，即非法获取个人信息，包括其通讯、银行、网络交易以及个人身份等相关信息。主要有以下几种行为方式模型。

第一种行为方式：

图 1-1

此种方式，是指行为人获取信息的方式是利用信息收集处理者的信息储存系统漏洞，对相关信息进行分析处理之后，对被害人实施诈骗行为。但是这种方式，信息收集及处理者获取用户的信息是经过用户授权，并未违法，只是疏于管理或者系统不完善，而导致用户信息泄露，用于不法行为。而且信息的收集及处理者没有故意提供用户信息用于不法用途，缺乏主观要件，不构成犯罪，无需承担刑事责任。

第二种行为方式：

图 1-2

此种方式与第一种方式的区别在于，其从信息收集处理者获取信息的方式不同，是信息收集及处理者非法向其提供。根据信息收集及处理者参与犯罪行为人后续诈骗行为的不同，可能有以下三种行为结果：①不参与后续犯罪行为，但是知道或者应该知道后续行为人使用信息的用途，而非法向其提供以及出售用户个人信息，可能构成诈骗罪的帮助犯[4]；②与后续的犯罪行为人有共谋行为而向其非法提供个人信息，可能构成诈骗罪的帮助犯；③信息收集及处理者将信息去识别化之后，向犯罪行为人非法提供及出售信息，可能构成侵犯公民个人信息罪。

第三种行为方式：

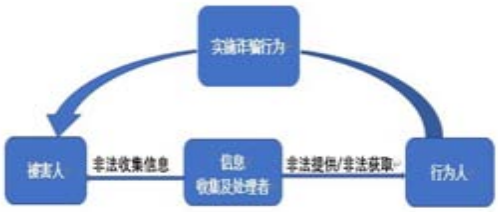

图 1-3

此种行为方式是指获取信息的最初源头就是非法的，整条信息产业链条都属于违法行为，信息收集及处理者可能构成侵犯公民个人信息罪，而犯罪行为人构成诈骗罪。

第四种行为方式：

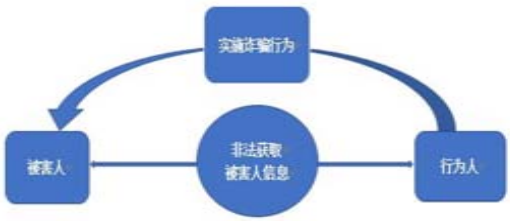

图 1-4

此种行为方式，是比较直接的方式，犯罪行为人一般通过“钓鱼”链接，利用被害人贪图便宜的心理，诱使被害人一步一步的授权其手机权限系统，然后通过算法机制悄悄的获取被害人的个人信息，再经过算法进行运算分析，得出分析报告，基于报告的基础开始逐步诱使被害人产生错误的认识，让其在错误认识下处分财物。此种方式目前已经开始下降，因为针对不同的被害人都需要从获取其信息阶段开始实施行为，其具有周期较长、效率较慢、工作量较大，但成功率较高的特征。

（2）以高端技术工具为主要媒介

电信网络诈骗犯罪区别于传统诈骗罪之处，就在于其犯罪行为实施具有高度的非接触式特点，往往呈现出跨省、跨境的形式诈骗。尤其是基于当前数据传输、数据工具、数据获取以及数据处理高度发达，诈骗犯罪分子往往都是通过各种通讯工具于受害群体建立通讯连接。目前中国境内的移动通信监测较为严格，于是大量的犯罪分子前往境外，如越南、缅甸等东南亚国家。缅甸北部针对中国境内实施诈骗犯罪活动尤其猖獗，由于具有跨境的特点，让中国警方难以打击犯罪行为。比如电信网络诈骗犯罪利用技术实现 GOIP 设备与 SIM 卡的分离，即使某一个环节被公安机关打掉，其犯罪的通讯线路也不会因此中断。此外，因为诈骗犯罪分子已然获取被害人的相关个人信息，可以根据被害人的信息塑造假身份对被害人实施长期的诈骗活动。典型的如“杀猪盘”。

（3）以协作分工为主要形式

信息技术的介入和被害人个人信息重要性使得网络诈骗犯罪无法独立完成，必然需要多方的配合。在传统环境之下，单独犯罪是主要的表现形式，以共同犯罪为例外的。但在数据信息新时代之下，以共同犯罪为常态，单独犯罪为例外。人民法院曾统计每一网络犯罪案件平均涉及 2.73 名犯罪嫌疑人，尤其是网络诈骗犯罪呈现出地域化、家族化以及公司化的特点。其涉及的犯罪行为人较多，主要是因为如需实现正犯（诈骗罪）的目的，必然需要引入互联网接入、服务器托管以及资金结算等其他帮助行为，这也是关联犯罪频发的因素。

2 电信网络诈骗犯罪中公民个人信息保护存在的问题

《个人信息保护法》的出台与实施，有效的实现了对公民个人信息的保障，也对打击电信网络诈骗犯罪活动提供法律上的帮助。但是碍于其作用和与其他法律法规之间联动性不足的局限性，对于电信网络诈骗的治理尚存在一些短板。

2.1 公民个人信息保护运行制度的缺失

2017 年颁布施行的《网络安全法》第四十条规定网络运营商需要严格的保守已收集到的用户信息，也赋予其应当建立相应的用户信息保密制度的责任[5]。而且这一立法思想在《个人信息保护法》中也得到了体现。但是当前大数据规制的“真空”出现，个人信息数据未得到有效监管。主要原因是由于数字信息时代的到来，科技、互联技术、大数据技术的高速发展，个人信息的内容不断外扩，从基本的生理信息到思想信息；从个体信息到社交信息；从现实信息到虚拟信息。个人信息的范围、内容及概念不断外延，在数据信息时代无处不在，而且以公众无法触摸、无法识别的方式被存储、传播以及处理。

个人信息管理混乱，无法得到有效保护。数字信息时代，个人信息的存储、处理发生划时代的变化。在许多涉及到个人信息存储、处理的企业公司没有建立完善的个人信息保护制度，存在过度收集、处理或者随意存储、使用等现象，而且有些公司存在超范围使用获取到的个人信息，严重侵犯公民的人身、财产权益。从前文可知，电信网络诈骗犯罪具有产业链的特点。通过从黑色产业中获取个人信息只是其中的一部分，对实施诈骗行为、骗取转账以及洗钱行为，仍然难以有较为有效的手段或方式进行规制。

2.2 电信网络诈骗犯罪侵犯个人信息的刑法适用问题

网络电信诈骗犯罪往往会对公民的个人信息也进行侵犯，虽然我国《刑法修正案（七）》增设了侵犯公民个人信息罪，但是在认定是否构成侵犯公民个人信息罪诸多方面还有着讨论。比如对个人信息处理者、提供者、收集者的处理方面，是否应该按照共同犯罪处理。在此问题上，主要有三种观点，一是按照共同犯罪处理，一条线打击；二是不按共犯处理，区别对待；三是看前面侵犯个人信息的行为是否与后面的犯罪行为具有紧密的关联性，如果有紧密关联性就按照共犯处理，如果没有就按照分别定罪的思维处理。

由于数字信息时代，网络社会具有扁平化的特点，犯罪的行为方式发生了巨大的改变，在电信网络诈骗犯罪这样的网络犯罪类型中，形成了犯罪产业链，很多犯罪参与者不具同一的犯罪目的，而是各自实施自己的犯罪行为，达到自己的犯罪目的，不能对某一犯罪链条上的所有行为主体产生支配，这就无法确定“正犯行为”、“正犯身份”。或者说是各个行为阶段的实施者，就是其自身的正犯行为。比如典型的电信网络诈骗犯罪，侵犯公民个人

信息的行为者与实施电信网络诈骗犯罪的行为不同时，实施各自的行为时，他们也没有意思上的联络，没有共同的犯罪合意。于是有的学者将此类称为意思联络性消解，认为上下游犯罪是一种相互协作的犯罪关系。而且主要是基于交易关系走在一起，上游犯罪，主要专门从事非法获取个人信息，进行出售、非法处理，为下游的诈骗、绑架、抢劫等犯罪活动提供便利。而下游的电信网络诈骗犯罪，实质上就是诈骗犯罪，只是借助电信互联网这个平台和方式。两者行为之间已经把帮助行为与正犯行为进行了界别。但是此外，有某些犯罪集团，专门形成固定的网络电信诈骗犯罪产业链，实施的行为既包括非法收集个人信息进行处理，也包括后期的网络精准诈骗，这种犯罪因为上下游具有紧密的关联性，所以笔者认为，应该认定为诈骗罪的共同犯罪。

3 公民个人信息保护对策

3.1 信息处理上：积极承担责任

公民的个人信息是其人格利益的体现，在对个人信息进行收集、处理时必须严格坚持目的正当性，前述图 1-3 和 1-4 的模式之下，从源头上获取的方式已经不符合相关规定，都是非法获取公民的个人信息的行为，违反目的正当性原则，对于相关收集者以及处理应该及时勒令删除收集到的相关信息，进行整改。判断收集者获取信息的内容是否符合目的正当性，需个案判断，如：医药企业收集公民的年龄、性别、身体指标、饮食、运动等信息，用于分析公众的身体状况是比较合理的行为。判断时网信部门必须分析收集者收集的信息与其生产经营方式的关联程度，如其收集恋爱状况、网上交易、银行转账等信息就严重不符合其生产经营，便需对其收集信息的目的和用途作违法推定性判断。强调个人信息收集以及处理的目的正当性，主要是目的是以此种方式限制个人信息他用行为的发生和直接用于违法行为。

其次是要求信息收集及处理者必须遵循用户知情同意的原则之下。许多敏感个人信息的收集必须让用户在了解相关用途以及处理的方式之下，才能对该信息进行收集和处理。这就要求信息内容管理主体要主动履行法定义务，对用户的个人信息充分负责，主要包含两个方面的内容：

（1）数据安全保护义务

数据作为新型生产要素，是数字化、网络化、智能化的基础，已快速融入生产、分配、流通、消费和社会服务管理等各个环节，深刻改变着生产方式、生活方式和社会治理方式。我国数据市场化的现象比较深，而对其保护的依据主要是《数据安全法》和《个人信息保护法》。信息内容管理主体主动对收集到的个人数据、企业数据以及公共数据进行分级确权授权处理，主动与政府、其它企业以及社会建立协同治理体系，积极引入第三方安全评估机构来对数据信息的运行、处理流程进行评估，降低主观评估的弊端，更好的保障用户个人信息。而且企业数据处理是指收集、存储、使用、加工、传输、提供以及公开，不能狭义的将信息处理理解成特指信息加工。企业应该使用标准规范网络数据处理活动，从而落实《数据安全法》等相关法律对数据安全保护的要求，履行社会责任[3]。在这个环节，企业也可以引入第三方数据评估机构来认证或证明企业满足标准中提出的数据安全基线要求[4]。

（2）合法处理个人信息

《信息安全技术移动智能终端的移动互联网应用程序（App）个人信息处理活动管理指南》征求意见稿[5]规定，移动智能终端对应用程序个人信息处理活动的管理宜遵循以下原则：①透明公开，要以合理、显著的方式记录、提示应用程序处理个人信息情况，确保用户对应用程序个人信息处理行为的可感知，让应用程序获取任何权限的行为需得到用户的明确授权；②方便管理，向用户提供个人信息管理入口，确保用户能方便地允许或拒绝应用程序对个人信息的处理，使得用户可以随时查看应用程序所获取的个人信息内容和方式；③确保安全，确保用户安装安全的应用程序，以及其以安全的方式处理个人信息；④细致管控，对于移动智能终端上敏感度较高的个人信息，实施限制处理，敏感数据访问提示和控制；⑤合理适度，采取合理的手段管理其上个人信息，实现用户对个人信息管控的同时，避免对用户在使用应用程序的过程中造成干扰，影响用户的使用。要求企业必须将这五个原则落实于数据信息收集处理全过程之中，包括预装、安装、更新以及使用应用程序的各个环节。

3.2 司法上：建立打击网络诈骗犯罪的合作联动机制

网络诈骗犯罪活动具有产业链化的特点，除公安机关打击处理外，必然需要其它相关部门的合作、配合，才可能对电信网络诈骗犯罪活动从源头上打击处理，从而保障我国公民的人身权益与财产权益。

首先是，与网信部门通力合作。由于《个人信息保护法》规定履行信息保护的主体是网信部门，如前所述，对于犯罪行为，必须要移交公安机关查办处理。针对同一行为有多方行政主体共同，既有可能导致有的主体推脱责任，也可能导致我国行政资源的浪费。网信部门发现违法处理个人信息涉嫌电信网络诈骗犯罪的，应当及时将相关证据一同移送公安机关依法处理。因为电信网络犯罪的证明难度较大，对涉及相关证据的认定较为严格，而网信部门才是电子证据获取的最佳主体，保障证据的客观性、真实性以及可靠性。因此应当建立个人信息涉嫌违法犯罪的证据制度。除此之外，网信部门对于数据信息定位的技术手段较高，公安机关与此合作，可以精准定位电信网络诈骗犯罪获取信息的源头，能够有效对上游非法买卖、交易以及提供信息的行为进行处理。其次是，与金融机构携手合作。由于电信网络诈骗犯罪活动通过其高效的洗钱方式，让公安机关难以挽回公民的财产损失。所以公安机关应大力加强与金融机构的合作，严厉打击下游洗钱行为。各区域公安机关可以与金融机构建立风险账号名单，对帐号实施实时监控，及时阻断其洗钱途径。

3.3 信息管理上：跨境个人信息限制传输机制

数据信息跨境流动很大程度给个人信息保护带了巨大风险，建立个人敏感信息数据限制传输机制对维护公民人身权益与财产权益十分必要。《数据出境安全评估办法（征求意见稿）》[6]中对数据处理者的义务作出规定，但是对于境外的信息收集者采用非法手段获取中国境内的个人信息却没有相应的条文作出规制措施。《中华人民共和国数据安全法》[6]第二十四条对国家提出了建立数据安全审查制度，但其目的是保障国家安全，层次比较高，对于个人信息这一较低层次的保护客体却无法将其解释为国家安全信息，于是便无法在这一领域得到有效保障。基于现行生效的法律法规可以得出一个结论：虽然我国对个人信息出境有一定的限制，但只是对合法出境途径行为的信息输出者的出境信息审查以及境外信息接收者的二次传输行为作出义务性要求，而对于避开合理路径的传输行为，尚没有建立相应的打击处理制度。对于非法途径传输个人信息数据出境的行为，公安机关、网信部门以及三大通信运营商首先应携手合作，打造一个网络防火墙，阻断境外利用电子信息技术窃取境内公民个人信息；其次，对识别的信息异常传输行为，应及时进行安全、风险审查，在第一时间切断传输路径，以防止公民个人信息被非法传输出境[6]。最后是，要加快推进对数据信息出境的细节规定的立法进程，比如对出境数据信息的个人信息保护负责人、保护机构、处理规则以及个人信息主体的权利进行明确，以保障个人信息主体能够通过各种途径和法律依据对其权利进行救济。

参考文献

[1] 王利明.敏感个人信息保护的基本问题——以《民法典》和《个人信息保护法》的解释为背景[J].当代法学,2022,36(01):3-14.

[2] 赵连庆.公民个人信息安全的刑法保护——以电信网络诈骗案件频发为视角[J].学习与探索,2017(09):80-84.

[3] 程啸.论公开的个人信息处理的法律规制[J/OL].中国法学:1-20.

[4] 张希嘉.个人信息保护中网络服务提供者的刑事责任[J].三明学院学报,2018,35(01):27-31.

[5] 张智浩.公民个人信息保护现实困境与突破[J].洛阳理工学院学报(社会科学版),2021,36(01):54-62.

[6] 张奕欣,邢潇,张金平.评个人信息出境安全评估最新方案[J].信息安全与通信保密,2022(03):19-26.

收稿日期：2022 年 6 月 15 日
出刊日期：2022 年 7 月 25 日
引用本文：杨旭，温小惠，公民个人信息保护研究——基于电信网络诈骗犯罪视角[J], 2022, 2(2) : 20-25
DOI: 10.12208/j.sdr.20220030

检索信息：RCCSE 权威核心学术期刊数据库、中国知网（CNKI Scholar）、万方数据 （WANFANG DATA）、Google Scholar 等数据库收录期刊