法学进展
2021 年 10 月第 3 卷第 4 期

公民个人信息利用的合法范围

李霰坤

中南财经政法大学法律硕士教育中心，武汉

摘　要 | 随着科技发展，国家和社会开始认识到大数据存在的巨大效益，依托大量个人信息和数据分析技术，已成为许多行业拉动经济增长促进创新的重要动力，对信息的掌握和运用甚至成为国家竞争力的一部分。但对个人信息的保护和利用间往往存在矛盾，在当前环境下采取过于严格的个人信息安全保护策略并不现实，出于功利主义角度也不利于发挥大数据的科技优势，但在对个人信息数据收集过程中，由于数据收集者具有隐蔽性、虚拟性的特点，用户在不知情的情况下隐私权、名誉权等受到侵害，甚至泄露的个人信息被用于诈骗等其他犯罪对社会金融管理秩序也造成了严重侵害，其危害结果兼具个体性与公共性。应以保障个人信息安全为前提，严格规范对个人信息利用的前置条件，为大数据技术的应用创造相应空间，方能体现法律（刑法）与科技发展的良性互动。

关键词 | 公民个人信息；刑法保护；问题研究

一、公民个人信息的权利性质

个人信息可谓是当代最有价值的资源，对于企业可以利用它产生丰厚的商业利润，对于政府可以利用它为决策提供依据，提高公共管理的效率与效益。①

作者简介：李霰坤，中南财经政法大学硕士，研究方向：知识产权。E-mail：administrator@stu.zuel.edu.cn。
文章引用：李霰坤．公民个人信息利用的合法范围［J］．法学进展，2021，3（4）：245-252.
https://doi.org/10.35534/al.0304026

① 齐爱民．个人信息保护法总论——拯救信息社会中的人格［M］．北京：北京大学出版社，2009：19.

因为擅自披露、提供、非法买卖个人信息等违法行为带来的巨大收益使不少个人企业铤而走险，对此我国也不断加强对侵害公民个人信息行为的打击力度，自 2009 年 2 月 28 日《刑法修正案（七）》增设“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”两项罪名到《刑法修正案（九）》的“侵犯公民个人信息罪”，充分体现出立法者对公民个人信息保护的重视。

对于公民个人信息的范围，根据《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》第 1 条的定义，列举了十几种类型，即包括个人姓名、身份证号码、地址等常见的形式，也包括行踪轨迹、账号密码等。分析认为，法律所保护的公民个人信息需具备以下特征：

首先，能够通过该信息识别、定位到特定自然人。个人信息范围所包括的公民具体职业、单位、家庭住址等都可以概括为体现公民的社会角色信息。正是基于信息具有可识别性，不法分子才能够利用他人信息进行犯罪，如冒用他人信息注册信用卡进行诈骗或盗刷消费、非法担保。其次，是信息能够反映公民的社会生活状态。不仅包括酒店住宿记录、通话记录等能够直接体现公民社会活动的内容，也包括数信息间能够相互结合、印证，推断出公民生活行为的内容。最后，个人信息还需要具有一定价值属性。个人信息对公民自身具有无可替代的自用价值，如使用身份证购买机票、银行通过个人信息综合衡量偿债能力发放贷款。同时通过众多公民个人信息形成大数据，将会产生相应的商业价值。随着社会的发展以及科技的进步，个人信息价值逐步呈现出多样性的特点，与此同时侵权方式也更加复杂化。

结合法律规范和司法解释，主要通过事实层面的具体行为体现公民个人信息的内涵与外延，但对公民个人信息这一法律概念的权利属性并没有具体说明。对于公民个人信息属人格权或财产权或是新型独立权利？学界也一直争论不休，因为对个人信息的定性直接影响到侵犯公民个人信息罪所保护的法益，在法律条文不宜调整具体案件时，立足整体从法益处罚直接关系到出罪和入罪的标准。

学界主要有以下几种观点：（1）所有权说。该学说认为个人信息，比如姓名、肖像具有财产价值，属于无体物或无形财产，是特殊的物权或所有权客体[①]，但

① 张莉．个人信息权的法哲学论纲［J］．河北法学，2010（2）：139.

如果将个人信息定性为物权客体，当购买者以合法途径购买个人信息随后非法使用，权利主体难以采取私力救济，显然并不合适。（2）隐私权说。在许多对个人信息率先立法的国家，都将个人信息保护置于隐私权的框架下，比如美国设立信息隐私的概念，日本则扩充了隐私权概念的定义，从传统的被动保护私生活安宁权利适当放宽至对信息的主动保护[①]，我国也有学者提出可以采取该模式[②]。而且根据《民法典》人格权部分的第 1034 条之规定：个人信息中的私密信息，适用有关隐私权的规定，由此作为论据支撑个人信息的保护应当从属于隐私权的保护下。（3）具体人格权说。个人信息权作为一项具体人格权与隐私权之间存在的众多差异，个人信息权不能被隐私权完全涵盖，是一项独立权利。[③]

对此笔者认为将个人信息与隐私权两者并不能等同，也不存在完全的隶属关系。隐私权是法定的民事权利类型，个人信息界定为民事权益更为适宜。[④] 对个人信息的保护范围并不限于隐私权，不过隐私权仍是信息保护中最核心的部分。从需要法律保护的角度来看，对个人信息权保护力度较弱，对隐私权的保护较强，因为隐私权是人格尊严的核心部分；也就是说，对于不构成隐私内容的一般个人信息不需要权利主体的特许同意就可以收集、不公开使用，但对于涉及隐私的公民私密信息，应优先适用关于隐私权保护的法律制度。

二、现行法律对公民个人信息的保护范围

（一）具有狭义可识别性或者隐私性的内容

全国人大常委会在 2012 年通过的《关于加强网络信息保护的决定》，是我国首部关于个人信息保护的专门立法，并且也是首次对个人信息进行定义[⑤]。在其后发布的《关于依法惩处侵害公民个人信息犯罪活动的通知》则采取了概括

① 谢青．日本的个人信息保护法制及启示［J］．政治与法律，2006（6）：154.
② 马特．个人资料保护之辩［J］．苏州大学学报，2012（6）：84.
③ 王利明．论个人信息权的法律保护［J］．现代法学，2013（4）：62.
④ 张新宝．个人信息收集：告知同意原则适用的限制［J］．比较法研究，2019（6）.
⑤ “国家保护能够识别公民人身份和涉及公民个人隐私的电子信息”

https://doi.org/10.35534/al.0304026

＋列举模式[①]列举了包括证件号码、履历、电话号码等十几种，对于人们认识哪些信息属于能够识别公民个人身份给出了一定的方向，同时该同志还提到对于涉及公民个人隐私的信息、数据资料也属于公民个人信息的保护范畴，可见在最初的法律规范中，立法者将“可识别性”与“隐私性”作为公民个人信息的核心保护内容，可识别性用于确定信息所属的公民个人，并强调对个人具有重要意义的隐私予以保护。

（二）广义可识别性的内容

根据《网络安全法》第 76 条规定[②]，在对个人信息保护的范围中删除了有关隐私信息的内容，隐私性不再作为公民个人信息保护的范畴，同时对可识别性的外延有所扩大，由只能通过单独识别的“直接型可识别信息”，扩充到包括能够和其他信息结合的“间接型可识别信息”。就此可以推论出立法者认为个人信息权和隐私权属于交叉关系，两者保护范围重叠的部分就是个人敏感信息或者说私密信息，按照该分类，可将个人信息可以分为一般个人信息，比如姓名、年龄等和个人隐私信息，比如收入、家庭住址等，个人私密信息将受到个人信息权和隐私权的双重保护，当私密信息受到侵害时权利人可以就侵害公民个人信息和侵害隐私权择一提起诉讼。

（三）广义可识别性和个人身份信息的内容

在 2017 年发布的《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 1 条[③]，又对个人信息的保护范围进行了修改，首先扩充了对公民个

① “公民个人信息包括公民的姓名、年龄、有效证件号码、婚姻状况、工作单位、学历、履历、家庭住址、电话号码等能够识别公民个人身份或者涉及公民个人隐私的信息、数据资料。”

② “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自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。”

③ “刑法第 253 条之一规定的‘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。”

人信息主要类型的列举，增加了账号密码、财产状况、行踪轨迹三种类型。对此有学者认为财产状况严格意义上并不具有可识别性，同时也不属于单独识别或者结合识别特定自然人身份的信息，超出了既有法律对个人信息保护的范畴。[①] 并且如果将账号密码认定为属于与其他信息结合能够识别特定人的信息类型也存在一定问题，因为账号秘密虽绑定自然人有效证件号码等个人信息，但是实践中对网络诈骗对往往是通过账号密码直接窃取账号财产，而不是利用账号密码非法获取公民其他身份信息。对个人信息予以保护的依据就在于，因为通过信息能够识别到具体的自然人身份，如果未经许可获取、使用对个人有可能造成损害，而该解释实则是出于保护“账号密码”“财产状况”背后的财产权，所以对公民个人信息的概念有所扩张。

三、利用公民个人信息的合法范围分析

如前所述，个人信息的发展拓展了社会整体信息体量。法律在强调对个人信息保护的同时，也不能对信息的使用条件过于严苛，保护过度膨胀，应切合风险和功利视角，构建全新个人信息保护观念[②]。对此笔者认为在以下几种情况下，互联网企业或者国家可以合法利用共鸣的个人信息：

（一）对信息匿名化处理后的使用

前文中已经论证过，我国现有法律对个人信息的认定标准之一就是具有“可识别性”，首先要认定构成法律意义上的个人信息，才有可能在数据的流通运用中，违反国家相关法律规定，构成侵害公民个人信息罪或者承担其他行政、民事责任。如果流通的数据并不具有个人信息的特征，对数据的利用就不再受到现行法律的约束。因此，如果对数据进行去识别化处理，通过数据不能识别到特定自然人，此时信息就不再是个人信息。所谓匿名化处理，是数据保有者，

① 于志刚．“公民个人信息”的权利属性与刑法保护思路［J］．浙江社会科学，2017（10）：4-14+155．

② 高磊．网络时代数据隐私的搜查干预——从滴滴顺风车司机抢劫、强奸、杀人案切入［J］．安徽大学学报（哲学社会科学版），2019（3）：124．

https://doi.org/10.35534/al.0304026

通过采取技术手段，对数据进行筛查，对能有识别特定身份的数据信息进行删改，避免信息主体隐私泄露的风险。匿名化处理方式已得到多国法律认可，在日本在 2015 年《个人信息保护法》中，首次设立匿名加工信息的数据类型，[①] 根据该法第 2 条之规定，达到无法识别特定当事人程度的匿名加工信息，在确保不能被恢复至原始状态后，未经本人同意也可由数据处理方提供给第三方。

从刑法的角度论证，将匿名化处理作为数据使用的合法事由的依据在于：首先根据构成要件，通过匿名化技术处理的个人数据，不再具有可识别性、关联性的特征，即该数据成为了非个人信息，因此也谈不上涉及侵犯个人信息犯罪；其次从保护法益角度，处理后的信息不具有泄露公民隐私或者损害其他权益的可能性。

（二）信息主体知情同意

尽管学界对个人信息的定义不一，但公民个人应当对信息享有自决权是毫无争议的。根据 OECD（世界经济合作与发展组织）颁布的《关于隐私保护和个人数据跨境流通的指南》，个人信息收集应当取得信息主体的同意，并且不应收集与所需目的无关的数据。[②] 正如前文论证的，将个人信息权定义为具体人格权更适宜我国法律制度，从个人信息的性质出发，如果作为具体人格权，那么就应该可以由权利人本人决定是否对内容进行保护，基于主体的意思自治也可以在知情同意的情况下，允许他人利用。

虽则在实践中该制度仍存在种种问题，知情同意的个人信息保护难以落到实处，网络平台用户面对冗长复杂的隐私声明，通常都直接点击同意；并且许多网络平台在自身领域内形成垄断缺少替代产品，用户只能被迫同意才能享受产品或服务；同时，企业收集的个人信息范围远超提供服务的范围，对于这种非必要信息的收集用户通常并不知情。[③] 但这并不是否认知情同意原则的作用，

① 佐藤一郎．“ビッグデータと個人情報保護法：データシェアリングにおけるパーソナルデータの取り扱い”［J］．情报管理，2016（11）：828.

② 高富平．个人数据保护和利用国际规则：源流与趋势［M］．北京：法律出版社，2016：36.

③ 范为．大数据时代个人信息保护的路径重构［J］．环球法律评论，2016（5）：93.

正如有学者说道“知情同意原则之于个人信息权，如同意思自治原之于民法”[①]。并且实践中的知情同意原则地位并没有因其缺陷削而弱，反而不断完善扩充，引发相关的数据访问权与迁移权、删除权等一系列相关权利。

（三）价值位阶原则的适用

法律本就是对各种社会利益进行协调的制度，如果存在相互冲突的不同利益，就必须对法益的重要性进行衡量，选择保护价值更大的利益，此时对部分法益的牺牲具有正当性[②]。在个人信息保护中也不例外，如在医疗领域中，如果对公民个人医疗信息的使用具有紧迫性，并且受条件所限难以进行匿名化处理，并且不利用该个人信息对社会利益会造成不可避免的损失。特别是在传染病大规模爆发时，社会成员都面临着现实紧迫危险，比如此次的新冠疫情，在这种情况下，国家强制力要求公民个人使用健康码，追踪个人的生活轨迹，是出于国家安全和不特定多数人的健康，该利益明显较个人信息更为重要，因此在该情况下对公民个人信息的必要内容进行公示，应当被认为是适当的。

Legal Scope of the Use of Citizens' Personal Information

Li Maikun

Zhongnan University of Economics and Law LLM Education Center, Wuhan

Abstract: With the development of science and technology, the country

① 齐爱民．拯救信息社会中的人格［M］．北京：北京大学出版社，2009：259.

② 周啸天．“最小从属性说的提倡：以对合法行为的利用为中心”［J］．法律科学（西北政法大学学报），2015（6）：73.

https://doi.org/10.35534/al.0304026

and society begin to realize the huge benefits of big data. Relying on a large amount of personal information and data analysis technology, it has become an important driving force for many industries to drive economic growth and promote innovation. Mastering and using information has even become a part of national competitiveness. But the contradiction between the protection and use of personal information is often, in the current environment take too strictly personal information safety protection strategy is not reality, from Angle of utilitarianism is unfavorable to play big data technology advantage, but in the process of data collection of personal information, because the data collector has the characteristics of concealment, virtual sex, Users' right of privacy and reputation are infringed without their knowledge, and even the leaked personal information is used for fraud and other crimes, which also causes serious infringement on the social financial management order. The harmful results are both individual and public. In order to reflect the positive interaction between law (criminal law) and the development of science and technology, it is necessary to ensure the security of personal information, strictly regulate the preconditions for the use of personal information, and create corresponding space for the application of big data technology.

Key words: Citizens' personal information; Criminal law protection; research problem