

# 已公开个人信息的刑法保护

王华伟\*

**内容提要：**合理划定处理已公开个人信息行为的刑事责任边界，意义重大。二次授权分析方案没有准确理解司法解释的规定，导致处罚范围过宽，且难以说明为何区别对待初次获取行为和再次提供行为。合目的性考察路径虽然逻辑更加周延，但是个人信息公开的合目的性在实践中很难把握和判断；而且，在信息已经客观公开的场合，仍然对信息处理者科以合目的性要求和义务，可能会压缩信息自由的空间。一般可访问性标准在个人信息保护和信息自由保障之间取得了平衡，是相对客观明确且易于认定的标准。在个人信息权的法益论立场下，应在对已公开个人信息进行类型化分析的基础上，以信息的客观开放程度为标准，统一认定信息处理行为的刑事责任。在对处理已公开个人信息行为的合法性审查中，不应仅关注下游信息处理行为，更应反思上游信息公开标准的合理性。

**关键词：**已公开个人信息 二次授权 合目的性 一般可访问 客观开放程度

## 一、问题意识与司法实务概况

过去十余年间，侵犯公民个人信息罪的判例数量持续增加，相关法律适用难题亦逐渐凸显。其中，对于已公开个人信息〔1〕能否以及如何得到刑法保护，产生了越来越大的争议。近年来我国逐步建立了相关的信息公开制度，如2014年国务院颁布《企业信息公示暂行条例》，同年国家企业信用信息公示系统正式上线；最高人民法院于2016年发布《关于人民法院在互联网公布裁判文书的规定》（以下简称“在互联网公布裁判文书规定”），截至目前，中国裁判文书网已经公开上亿篇司法文书。在企业公开信息和司法公开信息中，不可避免会包含一些个人信息，因此，这些规范和制度的设立与发展会间接导致大量个人信息的公开。此外，随着互

\* 北京大学法学院助理教授。

本文是教育部人文社会科学研究青年基金项目“刑法罪量要素的理论建构与实务应用研究”（20YJC820045）的阶段成果。

〔1〕 较之于个人隐私，个人信息是否存在已公开与未公开的划分，概念上可能存有疑义。个人信息能否被公众自由访问和获取，存在开放程度上的差异，其法律保护规则也有所不同，故不论是在个人信息保护法第27条、民法典第1036条还是在学术文献中，都存在“公开个人信息”这一概念。

联网社会从 Web1.0 时代演变至 Web2.0、Web3.0 时代，用户生成内容（UGC）越来越丰富，人们在社交媒体（如微博、微信、脸书等）表达个性化信息的需求十分旺盛，这也造成网络中公开的个人信息数量越来越大。而且，被非法获取和处理的个人信息，也可能客观上处于被公开的状态。更重要的是，由于信息处理技术的不断发展和普及，从互联网海量数据中收集、筛选、配对个人信息变得不再困难，例如通过网络爬虫技术批量获取数据和信息。在没有进一步授权的情况下，行为人通过技术手段等对已公开个人信息实施收集、加工、销售、提供等行为能否构成侵犯公民个人信息罪，目前司法实务并无一致看法。

案例 1：2018 年 3 月，李某注册为企查查 VIP 会员。李某使用企查查软件批量下载企业信息后，将其编辑分类为全国各地的企业个人信息数据（含有公司名称、法人代表姓名、联系方式、公司地址、邮箱），以“全国企业数据公司数据黄页”等名义通过淘宝网店销售。李某和购买信息主要用于商业推广的 20 名买家，都被认定构成侵犯公民个人信息罪。<sup>〔2〕</sup>

案例 2：2020 年 5 月至 7 月，吴某在天眼查、企查查等网站下载公开的各地企业工商登记信息，梳理分类后共出售 1.8 万余条信息，获利 1 万余元。在检察机关的监督下，2021 年 1 月 7 日，公安机关对吴某解除取保候审，作出撤销案件的决定。<sup>〔3〕</sup>

案例 3：2016 年 1 月起，柯某开始运营“房利帮”网站。柯某通过现金激励吸引房产中介注册会员并提供上传真实业主房源信息（包含房屋门牌号及业主姓名、电话等），并安排员工冒充房产中介联系业主核实，最后将有效信息有偿提供给网站会员。法院认定该行为构成侵犯公民个人信息罪。<sup>〔4〕</sup>

案例 1、案例 2 的行为手段如出一辙，处理结果却完全不同。后者最终作撤案处理，而前者甚至将买家也通通入罪，这恰恰代表着目前司法实务中的两种对立立场。

在过去的司法实务中，行为人通过某些公开渠道获取企业登记信息，<sup>〔5〕</sup>从中整理、筛选出个人信息加以出售的，常常被法院判决构成侵犯公民个人信息罪。笔者在中国裁判文书网通过“企查查”“天眼查”等关键词甄别，即检索到此类案件 40 余起。<sup>〔6〕</sup>但是，司法实务中也存在与此不同的理解和做法。同时，已公开个人信息的刑法保护问题也面临诸多新的变数。其一，民法典正式生效，在法秩序统一性原理的视野下，民法典中有关个人信息的民事责任条款会在一定程度上影响刑事责任的认定。尤其是，民法典第 1036 条第 2 项规定：合理处理自然人自行公开的或者其他已经合法公开的信息，行为人不承担民事责任，但该自然人明确拒绝或者处理该信息侵害其重大利益的除外。其二，个人信息保护法已正式通过，其第 27 条对已公

〔2〕 参见江苏省扬州市中级人民法院（2020）苏 10 刑终 79 号刑事裁定书。

〔3〕 参见卢志坚、白翼轩、田竞：《出卖公开的企业信息谋利：检察机关认定行为人不构成犯罪》，《检察日报》2021 年 1 月 20 日第 1 版。

〔4〕 参见上海市金山区人民法院（2018）沪 0116 刑初 839 号刑事判决书。

〔5〕 比较典型的公开数据来源，官方渠道包括中国裁判文书网、中国执行信息公开网、国家企业信用信息公示系统等；私人渠道包括企查查、天眼查、启信宝等。

〔6〕 篇幅所限，仅列举较有代表性的部分案例。例如，上诉人提出，涉案信息可在对应商事主体的企业年报中查询获取，其已向社会大众公开，并由企查查、天眼查等商业网站向社会大众广泛传播，处理该信息无需取得二次授权（参见广东省佛山市中级人民法院（2021）粤 06 刑终 345 号刑事裁定书）。还有上诉人援引《人民法院报》刊载的发回重审的同类案件，认为企业公开信息中的自然人信息不受刑法保护（参见福建省泉州市中级人民法院（2020）闽 05 刑终 155 号刑事裁定书）。甚至有辩护人指出，上诉人的行为与企查查的行为一致，既然国家法律未规定企查查搜集、加工、整理、出售企业信息的行为是犯罪行为，那么也不应认定上诉人的行为是犯罪行为（参见江苏省宿迁市中级人民法院（2019）苏 13 刑终 32 号刑事裁定书）。

开个人信息的处理规则作了规定，这也要在刑事责任的判断中加以考虑。尤其应予以注意的是，正式通过的个人信息保护法最终推翻了此前草案一审稿、二审稿中有关处理已公开个人信息的规则。其三，以前述案例2为代表，部分司法机关处理该类案件的立场发生了一定转变。事实上，在侵犯公民个人信息罪的司法认定中，也存在一部分将企业公开信息中的个人信息予以排除的判例。<sup>〔7〕</sup> 前述案例3的情形又有不同，该案中业主虽然自愿向中介提供房产信息，但其公开范围和程度都有限，对此类情形应如何处理，也需要探讨。对已公开个人信息的处理，固然关乎公民个人信息权利的保护，另一方面也涉及能否营造一种自由获取、处理、流通信息的良好社会氛围。在目前理论与实务严重缺乏共识的情况下，亟需对已公开个人信息的刑法保护问题进行系统梳理，给出妥当且易于把握的处理标准。

## 二、二次授权分析方案及其不足

### （一）二次授权的逻辑展开

在过去的司法实践中，实务界常常认为，在个人信息已被公开的情况下，如果收集这些信息并再次向他人提供，需要获得权利人的二次授权，否则属于违反国家有关规定，有可能构成侵犯公民个人信息罪。二次授权分析思路的直接依据是2017年“两高”《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》（以下称“个人信息刑事案件解释”）第3条第2款。该款规定，未经被收集者同意，将合法收集的公民个人信息向他人提供的，属于刑法第253条之一规定的“提供公民个人信息”，但是经过处理无法识别特定个人且不能复原的除外。认定处理已公开个人信息行为构成侵犯公民个人信息罪的相当大一部分判例，正是依据该规定，认为行为人获取已公开个人信息后未再次取得被收集者的同意，因而构成“出售型”或“提供型”侵犯公民个人信息罪。<sup>〔8〕</sup>

在理论上，喻海松较早关注了处理已公开个人信息行为的刑事责任问题。他认为，由于相关信息已经公开，获取行为无需取得同意，需要探讨的只是获取已公开个人信息以后再次提供的可罚性，因为此时涉及是否有二次授权的问题。对此，他主张应区分自愿公开和非自愿公开两种情形，对于前者不宜认定构成犯罪，对于后者则有可能按侵犯公民个人信息罪论处。<sup>〔9〕</sup>

民法典正式生效以后，其第1036条第2项的规定使个别司法机关的立场开始发生转变。在前述案例2中，检察机关认为，公安机关按照“个人信息刑事案件解释”第3条第2款的规定认定吴某涉嫌侵犯公民个人信息罪，但是按照民法典第1036条第2项的规定，没有证据证明吴某出售合法公开信息的行为遭到权利人拒绝或侵害其重大利益，因此不应认定构成侵犯公民个人信息罪。<sup>〔10〕</sup> 喻海松也认为，民法典第1036条第2项的规定否定了二次授权规则，除非

〔7〕 参见吴心斌、温锦资：《公民个人信息刑法保护的例外》，《人民法院报》2018年6月21日第7版；广东省深圳市龙华区人民法院（2020）粤0309刑初727号刑事判决书；广东省广州市白云区人民法院（2020）粤0111刑初1554号刑事判决书；江苏省苏州市姑苏区人民法院（2018）苏0508刑初40号刑事判决书；安徽省合肥市庐阳区人民法院（2019）皖0103刑初327号刑事判决书。

〔8〕 参见福建省安溪县人民法院（2019）闽0524刑初397号刑事判决书；福建省安溪县人民法院（2018）闽0524刑初932号刑事判决书；河南省开封市顺河回族区人民法院（2019）豫0203刑初19号刑事判决书。

〔9〕 参见喻海松：《侵犯公民个人信息罪司法疑难之案解》，《人民司法（案例）》2018年第32期，第14页；喻海松：《侵犯公民个人信息罪的司法适用态势与争议焦点探析》，《法律适用》2018年第7期，第12页。

〔10〕 参见前引〔3〕，卢志坚等文。

权利人明确拒绝或相关获取、提供行为侵害了其重大利益，只要行为人获取、提供已公开个人信息的行为处于“合理”限度内，就不宜再认定为犯罪。<sup>[11]</sup>

上述观点的基本逻辑是，区别评价对已公开个人信息的获取行为和再次提供行为。获取已公开个人信息时，推定信息处理者取得了第一次概括授权，因而完全属于“个人信息刑事案件解释”所称的“合法收集个人信息”。但是，收集后再次提供已公开个人信息时，则不存在这种推定授权，需要权利人二次授权才能使信息处理行为正当化。不过，民法典第1036条第2项的规定对二次授权是否产生影响以及能够产生多大影响，还只是引起了初步讨论。

## （二）二次授权的理论不足

二次授权分析方案虽然在形式上能够找到“个人信息刑事案件解释”第3条第2款作为依据，但其面临诸多疑问。其一，对一次授权和二次授权进行区分，没有充分理由。讨论处理已公开个人信息行为的民事或刑事责任时，问题的关键是该行为是否侵犯了公民的个人信息权。是否侵犯了这一权利，核心判断标准之一是信息处理者是否取得了权利人的同意。但是，在权利人没有明确约定或作出说明的情况下，如何能区分出权利人授权的层次，不免让人疑惑。按照侵犯公民个人信息罪的相关规定，非法获取和非法提供是并列的两种基本行为类型，二者只是行为样态有所不同，法益侵害性上则无本质区别。针对已公开个人信息，如果认为二次提供行为侵犯了公民的个人信息权，那么一次收集行为何以能够完全合法，并未得到充分说明。事实上，对这类案件的处理，援引“个人信息刑事案件解释”第3条第2款的规定，本身就可能存在误读。“个人信息刑事案件解释”第3条只是对“提供公民个人信息”的内涵作了细化阐述，即其不仅包括非法收集后提供，也包括合法收集后未经同意提供。由此并不能推导出对已公开个人信息的收集一概合法，也不意味着对所收集的已公开个人信息进行再次提供必须取得权利人的同意。换言之，该条并未特别涉及对已公开个人信息的处理。<sup>[12]</sup>处理已公开个人信息行为的合法性认定，仍需结合其他规定进行实质性判断。

其二，二次授权的要求在实践中很难操作，容易压缩处理公开信息的空间。按照二次授权理论，行为人在处理已公开个人信息之前，需取得信息权利人再次授权，但这几乎不可能做到。一方面，在数字化时代，数据是海量存在的，已公开个人信息同样如此。另一方面，信息权利人数量庞大且极度分散，很难逐个取得再次授权。在实践中，像企查查、天眼查、启信宝这类规模和影响较大的信息服务提供商，往往通过网络爬虫技术从国家企业信用信息公示系统等网站高效爬取信息，经过处理后再次提供给公众。对于其中涉及的个人信息，这类企业显然无法挨个取得信息权利人的二次授权。如果严格遵守二次授权标准，大批信息服务提供商将很难完全合法地开展业务，处理公开信息的空间会被严重挤压。

其三，民法典第1036条第2项的含义及其对刑事责任认定的影响，没有得到深入阐述。该项规定能够免除信息处理者民事乃至刑事责任的基本前提是，行为人系“合理处理”已公开个人信息。但是，“合理处理”“侵害重大利益”等概念的内涵并不明确。例如，企业信息公开的主要目标是通过推动市场主体的知情权，为交易主体或规制机构提供更加丰富的决策信

[11] 参见喻海松：《〈民法典〉视域下侵犯公民个人信息罪的司法适用》，《北京航空航天大学学报（社会科学版）》2020年第6期，第7页。

[12] 对该条规定制定背景的说明，参见周加海、邹涛、喻海松：《〈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〉的理解与适用》，《人民司法（应用）》2017年第19期，第33页。

息,从而有效改善决策质量,<sup>[13]</sup>最终实现以信用为基础的公平竞争和交易安全。<sup>[14]</sup>通过国家企业信用信息公示系统或企查查、天眼查等平台,从已公开企业工商登记信息中“清洗”出个人信息,然后予以贩卖,是否可以被认定为“合理处理”或“侵害重大利益”,在当前并不清楚。尤其是对于上述规范,民法和刑法在评价上的关系及差异,值得进一步探讨。

### 三、合目的性考察路径及其难题

与二次授权分析方案不同,关于处理已公开个人信息行为的合法性问题,存在另外一种判断信息处理是否符合信息公开规范目的的考察路径。

#### (一) 合目的性考察的基本思路

在个人信息保护法正式出台前,草案一审稿、二审稿对已公开个人信息的处理规则,没有采取所谓二次授权的思路。例如,草案二审稿第28条规定:“个人信息处理者处理已公开的个人信息,应当符合该个人信息被公开时的用途,超出与该用途相关的合理范围的,应当依照本法规定取得个人同意。”<sup>[15]</sup>显然,这一规定并没有区分一次授权和二次授权,其整体性地要求,对已公开个人信息的处理(不论一次处理还是二次处理)都应符合信息被公开时的用途。从文义上分析,草案二审稿第28条中的“处理已公开的个人信息”应当包括一次“收集”已公开的个人信息。换言之,在未经个人同意的情况下,对已公开个人信息的收集并非当然合法,遑论二次提供行为。在理论上,周光权认为,依据民法典第1036条的规定,对从已公开企业信息中获取公民个人信息的行为一概作无罪处理,并不妥当,而应结合公开信息的目的和用途来思考。他指出,如果处理个人信息明显违背个人公开其信息的目的和用途,有可能构成侵犯公民个人信息罪;如果处理个人信息的行为与个人公开其信息的目的没有根本抵触,则不宜定罪。<sup>[16]</sup>

较之二次授权理论,合目的性考察路径逻辑上更加周延,结论也更为合理。其一,不再对一次获取行为和二次提供行为进行差异化评价,而是将二者统一,只要违背了信息公开的目的和用途,不论是一次获取还是二次提供,理论上都可能构成侵犯公民个人信息罪。其二,不再形式化地援引“个人信息刑事案件解释”第3条第2款,一概要求二次提供行为须取得被收集者同意,而是从侵犯公民个人信息罪的保护法益出发,树立合目的性判断的实质标准,为处理已公开个人信息行为提供了更多出罪的可能。其三,尝试对民法典第1036条的规定进行限定解释。如果简单援引民法典第1036条,对处理已公开个人信息行为一概出罪,也会面临对个人信息保护不力的局面。

#### (二) 合目的性考察的实践难题

其一,信息公开的目的和用途具有多元性、复杂性和模糊性。信息公开的场景极为多样,法律法规的强制性规定、权利人的自发行为、被不法分子非法披露,都是个人信息直接或间接公开的可能原因。即使在法律法规作出强制性要求的场合,信息公开的目的或用途也

[13] 参见王伟:《企业信息公示机制的逻辑与立法研究——兼论〈企业信息公示暂行条例〉的修法思路》,《首都师范大学学报(社会科学版)》2021年第1期,第52页。

[14] 参见湛中乐、赵玄:《信用监管的法治理想与现实——兼论〈企业信息公示暂行条例〉的实施要点》,《中国工商管理研究》2015年第5期,第27页。

[15] 草案一审稿第28条与草案二审稿第28条的规定类似。

[16] 参见周光权:《侵犯公民个人信息罪的行为对象》,《清华法学》2021年第3期,第37页,第40页。

不一定能准确认定,因此,要求信息处理行为符合该种目的或用途存在一定困难。例如,企业信息公开的主要目的是让公众了解企业的基本情况,从而促进公平竞争,维护交易安全。如果行为人筛选其中的个人信息用于商业推广、推销等,则很难说这种获取、处理行为具有合目的性。再如,虽然企业需要采购一定的产品或设备,但其通常有既定的采购渠道和流程,将已公开企业信息中的个人信息用于商业推广、推销,恐怕还是违背了企业信息公开的用途。而且实践中,行为人获取、提供已公开个人信息通常是为了牟利,对于这些信息最终被如何使用或处理并不关心,此时合目的性也不易判断。至于自愿公开个人信息的情形,权利主体的目的更加不明确。如网民在各种社交媒体上展示诸多个人信息,常常自己都不确定是出于什么目的,而宽泛的“社会交往目标”又难以起到实质的限定作用。

其二,主观的目的性与客观的公开性之间存在一定的内在冲突。固然,权利人可以主张,其公开个人信息具有特定的主观目的。然而,如果个人信息客观上处于人人皆可获取的一般化公开状态,将违背特定主观目的处理信息的行为都认定为民事侵权甚至刑事犯罪,并不十分妥当。一方面,除非是个人信息被非法公开,个人信息的客观公开和主观授权通常紧密关联在一起。通常情况下,信息的一般化公开就意味着默认他人无需另行授权即可获取和处理信息。另一方面,对信息获取和处理者来说,信息权利人公开其信息的主观目的很难判断。如果不符合这种主观目的处理已公开信息的行为都被认定为非法,信息处理行为的自由空间无疑会被极大地压缩。而且,如果采取合目的性标准,对于同样的获取已公开个人信息的行为,如果行为人的主观目的符合个人信息公开的目的则属合法,反之则构成犯罪,这相当于将侵犯公民个人信息罪在一定程度上转变为特殊的非法定目的犯,而这不同于以往对本罪的通常理解,也会给司法认定增加难度。换言之,如果客观上信息可以被一般化地开放获取,主观上又对行为人获取、处理信息作出目的性限制,则二者之间会发生一定冲突,不仅司法实务不好把握,普通民众也难以适从。

其三,以个人信息保护法草案二审稿第28条为代表的合目的性考察路径,实际上对已公开个人信息的处理采取了相当严格的标准。有观点认为,如果采取这种标准,一般性的“人肉搜索”行为将会被认定为违法行为。<sup>[17]</sup>在向来严格保护个人信息的欧洲,具有代表性的欧盟《通用数据保护条例》(GDPR)和德国联邦数据保护法也没有采取这种立法模式的明确先例,这种规定可能存在过度限缩已公开个人信息处理空间的风险,其实践合理性有待深入论证。为避免该规定与民法典不能衔接的情况,<sup>[18]</sup>在个人信息保护法正式通过时,立法者最终放弃了草案一审稿、二审稿关于已公开个人信息处理的规定,转而采取与民法典第1036条第2项基本相似的规定:“个人信息处理者可以在合理的范围内处理个人自行公开或者其他已经合法公开的个人信息;个人明确拒绝的除外。个人信息处理者处理已公开的个人信息,对个人权益有重大影响的,应当依照本法规定取得个人同意。”

#### 四、一般可访问性标准

如何确定处理已公开个人信息行为的责任边界,并非中国特有的难题。作为数据保护立法

[17] 参见李旻等:《详细解读〈中华人民共和国个人信息保护法(草案)〉》, <https://weibo.com/ttarticle/p/show?id=2309404564436424982614>, 2021年6月21日最后访问。

[18] 参见《全国人民代表大会宪法和法律委员会关于〈中华人民共和国个人信息保护法(草案)〉审议结果的报告》, <http://www.npc.gov.cn/npc/c30834/202108/a528d76d41c44f33980eaffe0e329ffe.shtml>, 2021年9月20日最后访问。

的先行者，德国如何应对这一问题，值得进行比较研究。

### （一）一般可访问性概念

德国有关个人信息刑法保护的条款以附属刑法的方式规定于德国联邦数据保护法。按照该法第 42 条的规定，在未经授权的情况下，对非一般可访问的个人数据进行传输、公开、处理、骗取，分别处以 3 年以下自由刑或罚金刑、2 年以下自由刑或罚金刑。该条的适格行为客体只能是“非一般可访问的个人数据”，如果处理的是“一般可访问的个人数据”则不可罚。这就涉及了处理已公开个人信息行为的刑事责任评价问题。事实上，在 2019 年修订德国联邦数据保护法之前，该法第 28 条第 1 款第 3 项曾明确规定，如果数据是一般可访问的，应当允许收集、存储、修改、传输或者为了实现自身商业目的而使用个人数据，除非数据主体排除其数据处理。

德国联邦数据保护法罪刑规范早期规定的行为客体是“非公开的”（nicht offenkundig）个人数据，后来统一为“非一般可访问的”（nicht allgemein zugänglich）个人数据，但其内涵并无本质变化。<sup>[19]</sup> 2019 年修订前的德国联邦数据保护法第 10 条第 5 项曾规定，“一般可访问性数据”是指任何人都可以使用的数据，不论是否需要预先登记、得到许可或者支付费用。德国联邦最高法院曾在一起利用 GPS 装置非法收集他人行动轨迹的案例中指出，“一般可访问性数据”是那些访问路径在法律上不受限制，可以被任何人获悉的数据。<sup>[20]</sup> 虽然 2019 年根据欧盟《通用数据保护条例》对德国联邦数据保护法作了大幅修订，删除了“一般可访问性数据”的上述条款，但是，在立法空缺的情况下沿用上述旧法背景下的理解，仍然是有意义的。<sup>[21]</sup> 目前理论上一般认为，“一般可访问性数据”是指数据可以被无限制数量的对象所获知，或者数据在没有特别的条件或努力限制的情况下即可被访问。<sup>[22]</sup> 具体而言，在报纸、杂志、广播、电视、开放网站等媒介可以获取的个人数据，具有一般可访问性；在社交媒体上公开的个人资料，则应区分不同情况。如果只是需要形式化的登记即可获取，或其可访问性并未被限定在特定人群范围内，则也属于一般可访问的个人数据。<sup>[23]</sup>

存在一定争议的是来自公共登记系统的个人数据。在较早的部分判例中，德国法院曾认为，按照德国道路交通安全法的要求保存于车辆登记系统的车辆和车主数据，在展示一定“正当利益”之后即可获取，因此这些数据不属于生活领域的秘密，不仅不符合德国刑法第 203 条侵害隐私罪的构成要件，也不被德国联邦数据保护法规定的侵犯个人数据犯罪所涵盖。这类数据被视为一种公开的数据，因而不处于侵犯个人数据犯罪的保护目标之内。<sup>[24]</sup> 持这种立场的判例此后受到了较多批判。学者指出，法院并未详细解释“正当利益”的实质法律限制，这种宽泛理解将导致传输、处理各种领域登记系统中个人数据的行为都不会受到刑事处罚。<sup>[25]</sup> 其后德国联邦最高法院完全否定了上述法院判决，认为这种解释会弱化相关法律规定的访问要

[19] Vgl. BT - Drs. 14/5793, S. 64.

[20] Vgl. BGH: GPS-gestütztes Erstellen persönlicher Bewegungsprofile durch Detektei, Neue Juristische Wochenschrift, Heft 34, 2013, S. 2533.

[21] Vgl. Dallmann/Busse, Verarbeitung von öffentlichen personenbezogenen Daten, Datenschutzrechtliche Voraussetzungen und Grenzen, Zeitschrift für Datenschutz, Heft 9, 2019, S. 395.

[22] Vgl. Ehmann, in Gola/Heckmann (Hrsg.), Bundesdatenschutzgesetz Kommentar, 13. Aufl., 2019, § 42, Rn. 9.

[23] Vgl. Brodowski/Nowak, in Wolff/ Brink (Hrsg.), BeckOK Datenschutzrecht, Aufl. 35, 2021, BDSG § 42, Rn. 26.

[24] Vgl. HansOLG Hamburg: Weitergabe von Fahrzeug- und Halterdaten, Neue Zeitschrift für Strafrecht, Heft 7, 1998, S. 358; BayObLG: Halterdaten als offenkundige Daten, Neue Juristische Wochenschrift, Heft 23, 1999, S. 1727.

[25] Vgl. Weichert, Datenschutzstrafrecht - ein zahnloser Tiger?, Neue Zeitschrift für Strafrecht, Heft 10, 1999, S. 491.

求。由于登记机构需审核正当利益（如为了法律强制、执行、对法律请求的满足与抗辩等而需要获取数据），登记机构不属于一般可访问的信息来源，所以车辆和车主数据并非一般可访问的数据。<sup>[26]</sup>按照目前理论上的通说，德国联邦中央登记系统、<sup>[27]</sup>土地登记系统、户籍登记系统、车辆与车主登记系统中的个人数据，由于需说明正当利益才可获取，故都属于非一般可访问数据，仍然要受到德国联邦数据保护法罪刑条款的保护。<sup>[28]</sup>相反，债务人目录、商事登记系统、社团登记系统，则属于一般可访问的信息来源。<sup>[29]</sup>

## （二）标准设定及其深层理由

可以认为，德国在确定处理已公开个人信息行为的刑事责任边界时，主要采取了一般可访问性的客观化标准，而非信息处理的合目的性考察路径。按照该标准，在数据具有客观可访问性的基础上，只有对数据设定了某种法律上的实质访问条件限制，该数据才可能属于非一般可访问性个人数据；如果没有这种实质性限制，则排除相关数据处理行为的刑事可罚性。较之于合目的性标准，在已公开数据的可处理范围上，一般可访问性标准更加宽松。

德国立法采取这样一种标准设定，实际上是考虑到个人数据保护与公民信息自由之间的平衡。按照德国基本法第5条第1款的规定，人人都有从一般可访问的来源（allgemein zugängliche Quellen）不受阻碍地获取信息的权利。如果将获取一般可访问信息的行为纳入刑法处罚范围，会面临侵犯基本权利的指摘。从保护法益的层面看，德国立法对个人数据（信息）进行这种“非一般可访问性”的限缩，是因为就个人信息自决权而言，对于已公开的数据不需要施以与非公开数据同样程度的保护，<sup>[30]</sup>因为收集、处理一般可知悉的数据原则上没有侵犯信息自决权。<sup>[31]</sup>

## 五、客观开放程度标准之提倡

关于个人信息的法律保护制度，不论刑法规范的构成要件亦或民法规范的具体内涵，中国和德国都存在较大差异。但是，德国法上的一般可访问性标准仍然为我们提供了从客观外在角度思考已公开个人信息刑法保护的参考思路。本文将部分吸收这一比较法视角，立足于我国个人信息法律保护框架，从法益辨析、类型划分和规范分析等维度，探索一种基于客观开放程度标准的刑事责任认定方案。

### （一）法益保护基点的辨析

我国的侵犯公民个人信息罪并不像德国法那样，将行为客体明确限定为非一般可访问的个人数据。因此，在我国刑法语境下探讨处理已公开个人信息行为的刑事责任问题，必须深入到保护法益的实质性判断，而目前对于侵犯公民个人信息罪的保护法益仍然存在较大争议。

#### 1. 隐私权标准

较早期的观点认为，侵犯公民个人信息罪的保护法益是隐私权；无法体现公民隐私性的信

[26] Vgl. BGH: Verletzung von Privatgeheimnissen - Fahrzeug- und Halterdaten, Neue Juristische Wochenschrift, Heft 3, 2003, S. 227.

[27] 德语为 Bundeszentralregister, 该系统主要登记法院刑事判决、某些行政机构的决定、无刑事责任能力司法记录、特别法庭调查结果等。

[28] Vgl. Brodowski/Nowak, in Wolff/ Brink (Hrsg.), BeckOK Datenschutzrecht, Aufl. 35, 2021, BDSG § 42, Rn. 27.

[29] Vgl. Wolff, in Wolff/Brink (Hrsg.), BeckOK Datenschutzrecht, Aufl. 23, 2015, BDSG § 28, Rn. 82. 1.

[30] Vgl. Brodowski/Nowak, in Wolff/Brink (Hrsg.), BeckOK Datenschutzrecht, Aufl. 35, 2021, BDSG § 42, Rn. 25.

[31] Vgl. Pätzelt, Zur Offenkundigkeit von Halterdaten, Neue Juristische Wochenschrift, Heft 44, 1999, S. 3247.



息不能成为本罪对象，如有的被起获信息仅有公民姓名和办公电话或者手机号码，这些在正常的网络媒体上往往都能查阅，有的省市还开通了身份证的查号业务，此类信息应当被排除在犯罪对象之外。<sup>[32]</sup>按照这种观点，只要是客观上已经公开的个人信息，便不可能再受到刑法保护。这种理解已经无法得到广泛认同。

其一，在信息处理技术迅猛发展的时代，隐私权路径不足以充分保护公民的信息相关权利。德国联邦最高法院早在上世纪80年代就已经意识到现代数据处理条件下人格自由发展所面临的威胁，从而提出了个人信息自决权概念。<sup>[33]</sup>理论上也认为，在现代技术条件下，对公开数据的相关处理也可能威胁到公民的自由，这是超越隐私权理论的重要原因。<sup>[34]</sup>我国学界的研究也对传统隐私权和新型个人信息权的差异，进行了全方位考察，<sup>[35]</sup>在隐私权之外承认独立的个人信息权得到了越来越多的认同。如学者所言，即便是公开的个人信息，个人也应当有一定的控制的权利，如知晓在多大程度上公开、向什么样的人公开，别人会出于怎样的目的利用这些信息等。<sup>[36]</sup>

其二，民法典人格权编第六章明确区分了隐私权的保护和个人信息权利的保护。一方面，民法典对“个人信息”采取了识别型定义而非隐私权定义。另一方面，立法说明材料明确指出个人信息与隐私是两个不同的概念，二者的判断标准、范围、保护方式等都不完全相同，因此对隐私权和个人信息保护分别作了规定。<sup>[37]</sup>显然，前置法对个人信息保护的基本立场，应当在刑法的适用中得到充分尊重。在民法典专门规定个人信息受法律保护背景下，不宜再认为侵犯公民个人信息罪仅保护公民的隐私权。

其三，隐私权概念的含义过于丰富，很难准确界定。甚至在某些极具影响力的理论主张中，隐私权概念的内涵已经接近于个人信息自决权的定义。例如，有学者主张，隐私权是指自主决定何时、用怎样的方式以及在何种程度上与别人交流自己信息的权利。<sup>[38]</sup>

## 2. 识别性标准

不同于隐私权标准，目前相当一部分判决采取了识别性标准。所谓识别性标准，是指不论个人信息是否客观上已经公开，只要该信息具备识别特定自然人身份的效能，即应受到刑法保护。<sup>[39]</sup>这种立场值得肯定之处在于，其明确否定了以隐私权为基础的狭义保护范围，紧紧围绕司法解释对公民个人信息的扩张性定义进行司法适用。然而问题在于，隐私性的缺失固然不一定影响公民个人信息的保护，但据此认为一切可以直接或间接识别公民个人身份的信息都应纳入刑法保护范围，则有失偏颇。<sup>[40]</sup>事实上，识别性标准只是认定侵犯公民个人信息行为刑

[32] 参见付强：《非法获取公民个人信息罪的认定》，《国家检察官学院学报》2014年第2期，第117页。

[33] Vgl. Volkszählung, BVerfGE 65, 1.

[34] 参见〔德〕乌尔里希·齐白：《全球风险社会与信息社会中的刑法：二十一世纪刑法模式的转换》，周遵友、江溯等译，中国法制出版社2012年版，第294页。

[35] 参见王利明：《论个人信息权的法律保护——以个人信息权与隐私权的界分为中心》，《现代法学》2013年第4期，第66页以下。

[36] 参见王利明：《论个人信息权在人格权法中的地位》，《苏州大学学报（哲学社会科学版）》2012年第6期，第73页。

[37] 参见黄薇主编：《中华人民共和国民法典人格权编解读》，中国法制出版社2020年版，第208页，第213页。

[38] See Alan Westin, *Privacy and Freedom*, Athenum, 1967, p. 7; 张民安主编：《隐私权的界定》，中山大学出版社2017年版，第10页。

[39] 参见江苏省南京市中级人民法院（2017）苏01刑终870号刑事裁定书；山东省淄博市临淄区人民法院（2018）鲁0305刑初82号刑事判决书；辽宁省沈阳经济技术开发区人民法院（2018）辽0191刑初418号刑事判决书。

[40] 参见陈峰：《公开的工商企业登记信息也可成为公民个人信息》，《人民司法（案例）》2018年第32期，第6页。

事责任的必要不充分条件。上述观点只是形式性地套用了相关规范对公民个人信息的定义，而没有进一步分析，在个人信息已经客观公开的场合，是否仍然存在实质的需保护性。要对该类行为进行刑事处罚，必须回答其侵犯了信息权利人的何种法益。同样，前文援引“个人信息刑事案件解释”第3条第2款规定的判决意见，也没有回答这一问题。因为，当个人信息已经客观公开时，是否还需要被收集者同意恰恰是理论分歧的根本。因此，在适用该规定之前，应先行处理好“客观公开”与“同意”之间的关系。

### 3. 个人信息权标准

随着对侵犯公民个人信息罪保护法益的深入讨论，尤其是民法典对个人信息权利的确立，隐私权说逐渐式微，个人信息权理论越来越成为有力学说。<sup>[41]</sup> 个人信息权体现为对个人信息的支配和自主决定。<sup>[42]</sup> 在此基本语境下，判断处理已公开个人信息行为的刑事可罚性的关键是，该行为是否仍然侵犯了公民的个人信息权。对此，周光权认为，法益处分自由本身也应包含在法益概念之中，因而个人公开其信息的目的、信息的用途属于法益本身的一部分；如果处理个人信息违背了个人公开信息的目的、信息的用途，则侵犯了个人信息权，有可能构成侵犯公民个人信息罪。<sup>[43]</sup> 其论证的内在逻辑是，当处理个人信息的行为违背了公开信息的目的和用途时，就不存在一种允许处理个人信息的有效同意，行为仍然具有法益侵害性和不法性。

在构成要件的语义射程范围内，围绕个人信息权是否受损这一实质标准来把握处理已公开个人信息行为的可罚性，无疑是非常正确的。但是，在个人信息公开的多数情形中，个人信息通常依照相关法律法规强制公开，或者按照个人意思自愿公开，此时难言对已公开个人信息的处理侵害了权利人的法益处分自由。

其一，在依照法律或相关规范强制公开个人信息时，只要该法律或规范没有对处理已公开个人信息设置额外要求或条件，原则上数据权利人的同意就已经失去了约束力。例如，按照个人信息保护法第13条的规定，为履行法定职责或者法定义务所必需，个人信息处理者处理个人信息不需要取得个人同意。同样，按照欧盟《通用数据保护条例》第6条第1款e项的规定，数据处理是基于公共利益而执行任务或数据控制者实施公务职权所必要的，处理行为合法。这一数据处理情形与基于权利人同意的情形并列，同样具有合法性。显然，强制公开部分信息通常服务于一定的法定职责或公共利益，如中国裁判文书网、国家企业信用信息公示系统所进行的信息公开即是如此。这意味着，通过权衡个人信息利益与公共利益，在制度层面对个人同意原则作了一定的限制。

其二，在个人依其真实意思自愿公开个人信息时，权利人的同意并不存在明显瑕疵，在其未特别申明限制条件时，客观上就已经给予不特定数据处理者以概括性授权。例如，欧盟《通用数据保护条例》第9条第2款e项规定，数据处理若涉及数据主体自己公开的个人数据，则第1款的个人数据禁止处理规范不再适用。如果权利人一方面在未明确限制授权的情况下一般性地公开其个人信息，另一方面又主张数据处理必须符合其某种特定目的，这会给不特定的数据处理者带来不确定的法律风险。

[41] 参见前引〔16〕，周光权文，第31页；劳东燕：《个人数据的刑法保护模式》，《比较法研究》2020年第5期，第49页；刘艳红：《侵犯公民个人信息罪法益：个人法益及新型权利之确证》，《中国刑事法杂志》2019年第5期，第19页；冀洋：《法益自决权与侵犯公民个人信息罪的司法边界》，《中国法学》2019年第4期，第66页。

[42] 参见王利明：《和而不同：隐私权与个人信息的规则界分和适用》，《法学评论》2021年第2期，第22页。

[43] 参见前引〔16〕，周光权文，第38页。

## （二）客观开放程度标准之展开

在评价处理已公开个人信息行为的可罚性时，为了兼顾个人信息权和公民信息自由的保护，同时注重法律适用的稳定性和可操作性，对侵犯公民个人信息罪法益侵害性的判断，采取相对客观化的标准更为妥当。

### 1. 已公开个人信息的类型化

根据个人信息公开的不同语境，已公开个人信息大体可分为如下三种类型：其一，违法公开的个人信息。未经信息权利人同意，非法获取、提供、散布公民个人信息的行为，可能会使个人信息事实上处于已公开状态。在个人信息已被他人违法公开、传播的场合，刑法对非法获取、提供这类信息的行为不予规制，显然不合理，对此下文将进一步论述。值得注意的是，不同于个人信息保护法草案二审稿第28条的规定，最终通过的个人信息保护法第27条、民法典第1036条第2项，都仅将免责对象限定在“个人自行公开的个人信息”和“其他已经合法公开的个人信息”两种类型。

其二，依法依规强制公开的个人信息。为了实现一定的公共利益，如提升司法透明与公正，强化企业信用与交易安全等，法律法规会在一定条件下强制公开相关信息。例如，2014年国务院颁布的《企业信息公示暂行条例》第6条规定，工商行政管理部门应当通过企业信用信息公示系统，公示其在履行职责过程中产生的注册登记、备案信息、动产抵押登记信息、股权出质登记信息、行政处罚信息等企业信息。该条例第8条规定，企业应当于每年1月1日至6月30日，通过企业信用信息公示系统向行政管理部门报送上一年度报告（包括企业通信地址、邮编、联系电话、电子邮箱等诸多信息），并向社会公示。再如，“在互联网公布裁判文书规定”第3条要求，法院作出的刑事、民事、行政判决书和裁定书等裁判文书，应当在互联网公布。该规定第11条更是指出，法院在互联网公布裁判文书，应当保留当事人、法定代理人的姓名、出生日期、性别、住所地所属县、区，以及委托代理人、辩护人的姓名、执业证号和律师事务所、基层法律服务机构名称、出生日期、性别、住所地所属县、区，以及与当事人的关系等信息。此外，2019年国务院修订的《不动产登记暂行条例》第23条规定，国务院国土资源主管部门应当会同有关部门建立统一的不动产登记信息管理基础平台。该条例第27条同时规定，权利人、利害关系人可以依法查询、复制不动产登记资料，不动产登记机构应当提供。实务中，向有关部门查询不动产权属信息被称为“拉产调”，是市场活动中十分常见的做法，而“产调”信息中就包含部分个人信息。可见，不动产登记信息在满足一定条件的情况下，也可能会被依法依规在一定范围内强制公开。

上述几类依法依规强制公开的信息中包含了一定的个人信息，未经特别授权对其进行收集、筛选、提供等处理行为的刑法性质，理论上争议较大。一方面，依法依规强制公开信息服务于特定的公共利益，涉及公共利益与个人利益的平衡。对此，我国个人信息保护法和欧盟《通用数据保护条例》都作了相关规定。另一方面，依法依规强制公开个人信息存在不同类型，公众获取相关信息的要求和条件存在差异，开放的范围也有所不同，因此不能一概而论。这一点将影响对相关信息处理行为的刑法评价，下文将进一步展开论述。

其三，权利人自愿公开的个人信息。在社交媒体成为日常生活基本组成部分的时代背景下，人们习惯于在网络公共空间展示一些个人信息。一方面，这些信息是开展一定社会交往的基础，有利于建立起初步的信任关系。例如，公开自己的姓名、出生年月、教育背景、职业、工作经历、联系方式等信息。另一方面，披露个人信息也属于展示自我与分享生活的一种方

式，是网络时代普遍存在的一种社会心理需求。例如，展示大量私人照片或视频，这其中就会涉及一部分个人信息且其访问路径不严格受限。当权利人将个人信息置于网络公共空间予以开放时，或许权利人并未充分重视对自身个人信息的保护，但其客观上同意了他人对数据的访问，行为人对这些信息的处理通常在法律上并未违背权利人的意志。

## 2. 客观开放程度标准的具体内涵

(1) 在对已公开个人信息进行类型化的基础上，笔者主张侧重信息的客观开放程度而非信息处理的合目的性，统一划定已公开个人信息处理者的刑事责任边界。之所以采取这一客观开放程度标准，主要基于以下考虑。

首先，客观开放程度标准以客观事实为基本判断素材，有助于司法实务准确把握。根据合目的性考察路径，在司法认定过程中，法官可以站在事后的立场，结合诸多客观事实、素材和证据，对合目的性进行判断。但是，难以否认的是，其判断对象是主观目的及其符合性，终究还是会给刑事责任的认定带来相当大的实际困难和不确定性。在当下信息时代，信息公开的多种多样，而且信息一旦客观公开，受众极为广泛，经常要面对各种复杂的处理情形，信息查询、个人猎奇、牟利、市场分析、商业推广、数据服务乃至违法犯罪等等都有可能发生。因此，在实践中，不仅权利人公开相关信息的目的不易确定，信息处理者获取、提供、处理信息的目的也难以查明，要实现二者的契合更是难上加难。

与合目的性考察不同，客观开放程度标准主要考察个人信息的实际存在状态，不论在判断方法上还是判断对象上，都采取客观化方案。例如，只要个人信息客观上处于完全开放状态，处理个人信息的行为原则上就推定为免责，只有在例外情况下才应承担责任，对此下文会进一步展开。在民事法领域，展开合目的性考察或许不失为一种可能的路径，<sup>[44]</sup>但以此作为确定是否发动刑事处罚的关键标准，则宜审慎为之。民事法思维注重权利义务的合理分配与平衡，刑法的制度设计则应首先考虑明确性和稳定性。

其次，信息公开不仅服务于某些公共利益，在宏观层面也与信息自由紧密联系在一起。例如，在德国基本法中，信息自由被视为广义言论自由的组成部分。<sup>[45]</sup>《世界人权宣言》第19条也指出，言论和表达自由包括通过任何媒介且不论国界，寻求、接受和传递信息和思想的自由。站在信息权利人的立场，当然应保护公民的个人信息权不受损害，但从数据处理者的角度看，也不能过度压缩其他公民自由获取已公开信息的空间。尤其不能否认，对已公开信息的收集处理客观上带来了很大的积极社会效益。收集、处理已公开信息，通常依赖网络爬虫类技术，但该技术只能识别 robots 协议这类客观外在声明，而无法对信息公开的主观目的进行判断。即使在民事侵权领域，一些信息服务提供商（如启信宝、汇法正信公司）在未经同意的情况下转载、利用中国裁判文书网（或北京法院审判信息网）公开的裁判文书，被文书中记载的当事人起诉个人信息侵权，法院几乎都基于司法公开、司法数据共有共享等公共利益考量，认为该类行为尚属合理处理范畴，从而否定了侵权行为的构成。<sup>[46]</sup>只有采纳一种客观化

[44] 参见程啸：《个人信息保护法理解与适用》，中国法制出版社2021年版，第253页以下。

[45] 参见张翔主编：《德国宪法案例选释（第2辑）：言论自由》，法律出版社2016年版，第221页。

[46] 在苏州贝尔塔公司（启信宝）与伊某人格权纠纷案中，虽然法院最终判决贝尔塔公司构成对伊某个人信息的非法公开使用，但法院仍然指出，在伊某联系贝尔塔公司要求删除相关文书前，尚不构成侵权（参见江苏省苏州市中级人民法院（2019）苏05民终4745号民事判决书）。在北京汇法正信公司与梁某网络侵权责任纠纷案中，法院则基于公共利益、社会经济利益与个人信息利益的平衡，直接认定转载行为不构成侵权（参见北京市第四中级人民法院（2021）京04民终71号民事判决书）。

的认定标准，这类常见的信息和数据处理行为才不至于总是在法律红线面前如履薄冰。而且，如果在已公开信息的访问、获取和提供过程中，需进行繁琐、复杂的二次授权或合目的性考察，社会整体的信息自由度和数据流转都可能显著下降。

最后，如果不确定统一标准，而是差异化对待获取、处理、再次提供已公开个人信息等行为，可能会引发法律适用上的不统一。在其他主客观条件相同的情况下，获取、处理、再次提供等行为在基本性质上并无本质差异。在明显不合理处理已公开个人信息的场合，只规制再次提供行为而放任初次获取行为，会人为形成处罚漏洞，对个人信息权的保护也过于滞后。而且，如果区别对待初次获取行为和再次提供行为，还要面临行为着手何时开始，初次获取行为是否存在预备、未遂等诸多难题。

(2) 判断处理已公开个人信息行为是否构成侵犯公民个人信息罪的关键在于，从实质上分析处理行为是否具有“非法性”以及是否“违反国家有关规定”。因此，前置法或前置规范判断成为确定该行为性质的关键。但是，关于已公开个人信息的处理，对前置规定的理解并不完全统一，对此可以总结为以下两种模式。

首先，免除同意模式。免除同意模式意味着，在处理个人信息时，个人信息的合法自愿公开状态原则上免除了信息权利人的现实同意要件。例如，2020年国家标准化管理委员会发布的《信息安全技术个人信息安全规范》第5.6条规定，所涉及的个人信息是个人信息主体自行向社会公众公开的，或从合法公开披露的信息中收集个人信息的，个人信息控制者收集、使用个人信息不必征得个人信息主体的授权同意。再如，2013年国务院颁布的《征信业管理条例》第13条规定：采集个人信息应当经信息主体本人同意，未经本人同意不得采集，但是依照法律、行政法规规定公开的信息除外；企业的董事、监事、高级管理人员与其履行职务相关的信息，不作为个人信息。<sup>[47]</sup>此外，民法典第1036条第1项规定，经自然人同意的，处理个人信息不承担民事责任；第2项则并列规定合理处理自然人自行公开的或者其他已经合法公开的信息，处理者通常不承担民事责任。个人信息保护法第27条基本采取了类似表述。这些规定的共同特征是，当个人信息自愿或合法公开时，概括推定权利人对处理这些信息的同意效力，因此，在没有实际同意的场合也能达到免责效果；除非出现某些例外情况（如权利人明确拒绝或侵犯权利人重大利益），处理者原则上无需承担责任。

其次，符合用途模式。符合用途模式要求，对已公开个人信息的处理应当符合个人信息被公开时的用途，其典型体现就是个人信息保护法草案一审稿、二审稿第28条。较之于免除同意模式，符合用途模式对已公开个人信息的处理提出了更严格的要求，其要求个人信息处理者应当严格遵守个人信息被公开时的用途，即使这一用途本身不明确，个人信息处理者也须合理、谨慎处理已公开个人信息。从个人信息保护法草案一审稿、二审稿第28条的表述推断，识别已公开个人信息的用途的义务事实上被施加给了信息处理者。相应地，按照该草案一审稿第62条、二审稿第65条的规定，如果违反了这种义务，信息处理者可能面临警告、没收违法所得和罚款等处罚。以此为基础，甚至可以进一步推导出处理者的刑事责任。

对于处理已公开个人信息的行为，如果采取免除同意模式，并对“合理处理”要件作相

[47] 2014年最高人民法院《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》第12条也曾间接提到，网络用户或者网络服务提供者利用网络公开个人隐私和其他个人信息，造成他人损害，应承担侵权责任，但是自然人自行在网络上公开的信息或者其他已经合法公开的个人信息、以合法渠道获取的个人信息除外。

对宽松的解释,则出罪空间较大;如果采取符合用途模式,则入罪的可能性较大。当然,从解释论上说,如果将“违背个人信息被公开时的用途”等同于“不合理处理”,两种模式将得以兼容。<sup>[48]</sup>但是,如此理解显然是对民法典第1036条第2项的免责规定作了极大限缩。在海量且一般性开放的数据和信息面前,要判断和确认个人信息公开的用途和现实合目的性,不论是在信息权利人一侧,还是在信息处理者一侧,都面临技术层面和规范层面的困难。如果对信息处理者直接或间接科以甄别信息公开用途的义务,则会大大压缩信息处理的自由空间。

总而言之,在确定侵犯公民个人信息罪的前置法或前置规范依据时,应当以民法典第1036条第2项、个人信息保护法第27条所设定的免除同意模式为基础。处理自行公开和已经合法公开的个人信息,原则上无需额外获得权利人同意,只有在例外情形下该推定同意才失去效力。当然,这并不意味着上述规定就是“免责令”“免罪符”,而是应当通过平衡保护个人信息权和公众信息自由的方式,妥善界定“合理处理”的内涵。对此,民法学界尚未展开充分研究。而就刑事责任认定来说,应当从两个层次理解上述前置法规范:一是在法秩序统一性原理的视野下,立足于缓和的违法一元论立场,应当认可前置法中免责规范对刑事责任认定的影响。具言之,民法中不认定构成侵权、无需承担责任的处理已公开个人信息行为,不应作为犯罪处理。二是考虑到刑法与民法的相对性关系,<sup>[49]</sup>对上述免责规范,刑法可以作出与前置法不同的理解。鉴于刑法相对保守和克制的基本性质,尤其是刑事处罚对数据要素市场发展所可能带来的外溢效应,刑法对免责规范的理解可以比前置法更为宽松。如果对处理已公开个人信息行为广泛入罪,当前活跃的信息服务提供商如天眼查、企查查等的经营行为恐怕会受到极大影响。

有观点主张,原则上只要法律法规未明确禁止的处理已公开个人信息行为,均可认定为“合理处理”。<sup>[50]</sup>至少在刑法领域,这种宽松解释值得肯定。在个人信息客观上已自行或合法公开的场合,刑法意义上的“不合理处理”,主要就是指“自然人明确拒绝”和“处理行为侵害权利人重大利益”。在此类情形下,仍然需要刑法例外地予以保护,这与个人信息权的法定定位和理论逻辑并无根本冲突。民法典第1036条第2项、个人信息保护法第27条事实上并非对个人信息权利自决的否定,其设定个人信息处理行为免责事由的原因在于“个人自行公开”代表了主体的概括同意,“合法公开”则是基于公共利益考量适度限制个人信息自决的范围。反之,“自然人明确拒绝”意味着信息权利人否定了被推定的概括同意,此时仍然违背其意愿处理个人信息就侵犯了个人信息权,不再属于“合理处理”的范畴。“处理行为侵害权利人重大利益”则是指信息处理行为有损自然人的生命、身体、自由、财产等利益,此时不仅推定的概括同意失效,公共利益考量也不再处于优先位置。例如,通过对已公开信息的处理进行人格画像,对公民进行种族、性别歧视。<sup>[51]</sup>

除此之外,利用已公开个人信息进行业务拓展、商业推广,以营利方式为他人提供信息查询、整理服务等,仍可在刑法上解释为“合理处理”。有观点认为,利用自然人自行对外公开的电话号码向其发送垃圾短信,属于侵害重大利益。<sup>[52]</sup>这种判断在民法领域或许可以成立,

[48] 参见前引[16],周光权文,第38页。

[49] 参见于改之:《法域冲突的排除:立场、规则与适用》,《中国法学》2018年第4期,第88页以下。

[50] 参见前引[11],喻海松文,第7页。

[51] 参进程啸:《论我国民法典中的个人信息合理使用制度》,《中外法学》2020年第4期,第1016页。

[52] 参见前引[37],黄薇主编书,第221页。

但在刑法上不宜一概如此认定，因为很多时候业务拓展、商业推广与发送垃圾短信之间的界限非常模糊。而且，刑法上对“侵害重大利益”的理解应与民法上的解释有所区别。侵犯公民个人信息罪被规定在刑法分则第四章“侵犯人身权利罪”中，理论上认为该罪保护的个人信息权应当与行动自由、生命身体安全、财产等存在一定联系。<sup>[53]</sup>另外，对于无法查明信息处理行为直接后果的情况，例如单纯将已公开个人信息向不特定主体提供或出售，也应作存疑时有利于信息处理者的解释。

(3) 根据以信息客观开放程度为基本判断依据的客观公开标准，针对不同类型的已公开个人信息，可以进行如下具体操作。

首先，完全开放个人信息的处理。所谓完全开放的个人信息，是指客观上没有任何条件限制，或仅有一些形式上的条件限制，不特定主体皆可获取的个人信息。这类信息既可能是信息权利人自行公开，也可能是基于法定理由强制公开。如果个人信息的访问需满足一定的形式性条件，如快速注册账号、通过验证码验证，也仍然属于完全开放的个人信息。这种形式性的限制条件只是出于一定技术性考虑而设，其既未否定信息权利人的概括性同意，也未否定依法依规强制公开信息所考量的公共利益。

对完全开放个人信息的处理（不论是初次获取还是再次提供），实际上获得了基于个人同意或法律法规推定的概括授权，原则上符合民法典第1036条第2项和个人信息保护法第27条规定的免责条件，通常不会侵犯个人信息权，无需刑法干预。因此，从中国裁判文书网、天眼查、企查查等平台下载数据后再次提供的行为，一般不宜作为犯罪处理。从本质上看，这类行为只是居间促进了完全开放数据的进一步流通，即使没有这类行为，用户仍然可以获取这些数据，只是效率较低而已。例如，在前文案例1中，买家如果不通过李某提供的数据销售服务，仍然可以自己在企查查平台获取用于商业推广的目标数据，只不过更加耗时耗力。既然人人皆可访问、获取这些包含一定个人信息的数据，何以居间者的介入就彻底改变了行为的性质？事实上，目前具有相当影响力的民事判例认为，为了获取广告、投资等收益对已公开信息（其中包括个人信息）进行商业化利用，具有盈利目的，并不意味着该利用行为就是不正当行为。<sup>[54]</sup>既然如此，对于行为性质类似的前文案例1，就更无必要草率发动刑事处罚，因此前文案例2中司法机关注重协调刑民关系的审慎立场就值得肯定。对于这类信息处理行为，并非完全放任不管，而是通过民法或行政法手段予以应对和规制便已足够。例如，指示权利人向相关裁判文书公布单位反映解决，或赋予公民请求删除相关已公开个人信息的权利。<sup>[55]</sup>这些都是可以探讨的可行方案。

但是，在自然人明确拒绝或者信息处理行为侵犯权利人重大利益时，相关免责规范不再适用，处理已公开个人信息的行为就可能例外地具有刑事可罚性。例如，从企查查、天眼查等平台下载数据，筛选出个人信息用于实施诈骗。对于这类案件，认定构成诈骗罪和侵犯公民个人信息罪且数罪并罚，<sup>[56]</sup>是基本妥当的。即使诈骗未能着手或得逞，或者诈骗数额不明，不易

[53] 参见前引〔16〕，周光权文，第31页；马永强：《侵犯公民个人信息罪的法益属性确证》，《环球法律评论》2021年第2期，第112页。

[54] 参见前引〔46〕，（2021）京04民终71号民事判决书；前引〔46〕，（2019）苏05民终4745号民事判决书。

[55] 同上。

[56] 参见广西壮族自治区南宁市中级人民法院（2020）桂01刑终372号刑事裁定书；广西壮族自治区宾阳县人民法院（2018）桂0126刑初493号刑事判决书。

认定构成诈骗罪，至少也可以认定构成侵犯公民个人信息罪。<sup>[57]</sup>

其次，限制开放个人信息的处理。所谓限制开放的个人信息的处理，是指客观上存在一些实质性限制条件，如具有特定主体资格或特定权利关系才可访问的个人信息。限制开放的个人信息的处理并未向不特定主体无条件地一般性开放，因此，不论是在自愿授权还是法律法规强制的层面，都没有擅自处理这类信息的正当性。

例如，为了促进交易安全，在很多国家房产信息都可以通过一定渠道开放查询。房产信息不仅包含一些个人敏感信息（如姓名、出生日期、身份证号码、住址等），而且本身就可以部分体现信息权利人的财产状况。按照2019年修订的自然资源部《不动产登记资料查询暂行办法》第8条的规定，不动产权利人、利害关系人申请查询不动产登记资料，应当提交查询申请书（包括查询主体、目的、内容等）以及不动产权利人、利害关系人的身份证明资料。这一规定不仅提出了主体资格限制，也提出了实质性申请条件，因此房产信息属于限制开放的个人信息的处理。如果违反相关条件和程序获取、提供这类信息，就可能构成侵犯公民个人信息罪。如果公民只是在一定范围内授权房屋中介使用房产信息，则该类信息仍处于限制开放状态，需要刑法予以保护。在前文案例3中，行为人诱导房屋中介未经授权超越特定使用范围上传、提供与房产相关的个人信息，并将这些信息有偿提供给不特定他人，就仍然构成侵犯公民个人信息罪。<sup>[58]</sup>不过，房产信息的开放程度和状态并非一成不变，其取决于特定时空条件和不同社会背景下的法律法规规定。例如，按照2006年建设部曾颁布的《房屋权属登记信息查询暂行办法》（已失效）第7条、第11条的规定，查询房产信息的条件就非常宽松，此时房产信息的开放性程度就比较高。在世界范围内，有的国家采取了完全、无限制地公开不动产登记信息的模式（如俄罗斯），有的国家则采取有限度地公开不动产登记信息的模式（如德国）。<sup>[59]</sup>再如，社交媒体中网络用户有条件开放的个人信息的处理，也可能属于限制开放的个人信息的处理。若需添加好友或通过验证等才能查看网络用户的相关个人信息，则这部分信息的开放性实际上仍然被限制在较小范围内，相关信息仍应受到刑法保护。

最后，被违法公开个人信息的处理。不论客观上是完全开放还是限制开放，如果个人信息系被他人违法公开，则信息处理行为（包括获取和提供）仍应受到刑法规制。按照隐私权标准，“隐私一旦被披露就不再是隐私”，<sup>[60]</sup>被违法公开的个人信息的处理后续无法受到侵犯公民个人信息罪的保护。但从个人信息权的角度看，该权利的内涵十分丰富。民法典第1035条、第1037条直接或间接确认了公民个人信息的决定权、查阅权、复制权、更正权、删除权。<sup>[61]</sup>个人信息保护法第44条至第47条更是明确规定了知情权、决定权、查阅权、复制权、更正权、删除权等权利。除此之外，理论上认为个人信息权还可以包括占有权、保护权、锁定权等权

[57] 参见广西壮族自治区宾阳县人民法院（2018）桂0126刑初467号刑事判决书；广西壮族自治区宾阳县人民法院（2018）桂0126刑初487号刑事判决书；广西壮族自治区田林县人民法院（2019）桂1029刑初43号刑事判决书。

[58] 最高人民法院第140号指导案例的裁判要旨指出，业主房源信息属于公民个人信息，未经信息主体另行授权，非法获取、出售限定使用范围的业主房源信息，系侵犯公民个人信息的行为。前文案例3的审理经过和判决意见，参见前引〔4〕，（2018）沪0116刑初839号刑事判决书；舒平锋、金淑琴：《未经同意传播房源信息构成侵犯公民个人信息罪》，《人民司法（案例）》2020年第23期，第44页。

[59] 参见冯骏、许云勇：《不动产登记信息公开是现代民法的必然要求——对〈房屋权属登记信息查询暂行办法〉的简要说明》，《中国房地产》2007年第2期，第45页。

[60] 前引〔35〕，王利明文，第67页。

[61] 参见吕炳斌：《论〈民法典〉个人信息保护规则蕴含的权利——以分析法学的权利理论为视角》，《比较法研究》2021年第3期，第40页。



利。<sup>[62]</sup> 这些权利很大程度上突破了隐私权的范围，即使个人信息已被违法公开，公民仍然享有其中一项或多项权利，相关的再次侵害行为仍然要受到刑法规制。因此，如果行为人明知是他人违法公开的个人信息而予以非法获取、提供，情节严重的，具有刑事可罚性。在司法实务中，从微信群、QQ群、论坛等网络媒介下载被违法公开的个人信息，通常认定构成侵犯公民个人信息罪。<sup>[63]</sup>

## 六、信息公开标准之反思

不可否认，处理已公开个人信息领域出现的乱象，对公民个人信息的法律保护形成了挑战。但是，问题的成因绝非仅来自信息处理者。在高度发达的信息社会，信息处理的场景和层次极为复杂，并且常常处在不确定的动态流转过程中，信息一旦一般性公开，要确保其处理完全符合预设的特定目标或用途会相当困难。因此，与其将关注重点仅仅放在下游对已公开个人信息的处理上，不如进一步反思现有制度对相关个人信息予以公开的做法是否真正合理合法。换言之，合目的性考察最好前移至信息公开相对集中的上游，而非信息处理流程相对分散的下游。以中国裁判文书网的信息公开机制为例，2014年至2019年公布刑事、民事裁判文书3544万余篇，其中个人信息未被模糊化处理的文书接近609万篇，占比约17%。<sup>[64]</sup>之所以形成了这一颇为惊人的局面，一方面应归因于在裁判文书公开过程中未从观念上、技术上充分重视个人信息保护；另一方面，裁判文书信息公开标准本身的合理性也值得反思。

其一，司法公开注重形式性，实质目标定位不清晰。“在互联网公布裁判文书规定”指出，公开裁判文书的目的是落实审判公开原则，促进司法公正，提升司法公信力。然而，这些目标的实现主要依靠对裁判过程及其合理性的监督，而非简单披露当事人个人信息。司法公开的关注重点更应侧重司法权运行，而非（尤其是民事案件）当事人之间的争端本身。如果不强化裁判文书说理，将司法裁判的具体理由和逻辑公之于众，接受实质监督，公开再多的案件事实信息，对于提升司法公信力的价值也是有限的。诚如学者所言，相较法治发达国家，我国更加注重司法形式意义上的公开，在实质公开上却处于相对较低水平。<sup>[65]</sup>

其二，个人信息公开的范围是否符合比例性原则尚存疑问。虽然“在互联网公布裁判文书规定”已经在一定程度上考虑到司法信息公开与个人隐私保护之间的平衡，但在公开相关个人信息的范围上仍然值得反思。例如，“在互联网公布裁判文书规定”第8条对三类主体姓名的隐名处理作了规定。但是，民事案件中是否只有婚姻家庭、继承纠纷案件中的当事人及其法定代理人才应隐名处理，不无疑问。大量一般经济纠纷、债务纠纷案件中所涉个人隐私（如经济状况）应否保护，也须认真对待。再如，按照“在互联网公布裁判文书规定”第11条，除根据第8条进行隐名处理的，当事人、法定代理人、委托代理人、辩护人的诸多个人信息都应予以保留。问题在于，上述很多个人信息的公开并不能服务于司法公开、公正的目标追

[62] 参见王利明、杨立新、王轶、程啸：《民法学》，法律出版社2020年版，第914页。

[63] 参见广东省深圳市中级人民法院（2017）粤03刑终1719号刑事裁定书；广东省新兴县人民法院（2019）粤5321刑初58号刑事判决书；广东省深圳市宝安区人民法院（2017）粤0306刑初4930号刑事判决书。

[64] 参见邹邵坤、侯晓焱：《民法典时代我国公开裁判文书个人信息保护提升路径》，《法律适用》2020年第20期，第26页。

[65] 参见韩朝炜、朱瑞：《裁判文书上网与当事人隐私权保护的冲突与平衡》，《法律适用》2012年第4期，第96页。

求。例如，当事人、委托代理人、辩护人的出生日期、性别、住所地所属县、区是完全个人化的信息，和案件争议并无直接关系，也不是司法裁判结果所指向的对象，<sup>[66]</sup>实无公开的必要。比较而言，美国裁判文书“首部”中仅写明当事人姓名，并不出现性别、出生年月、住址等个人信息。<sup>[67]</sup>因此，裁判文书中个人信息公开范围的确定，应设立更加严格的实质关联性标准，否则会有违背个人信息公开比例性原则之嫌。<sup>[68]</sup>

其三，在基本理念上，裁判文书信息公开追求的仍然是个人隐私保护而非个人信息保护。“在互联网公布裁判文书规定”的相关条款表明，在裁判文书公开过程中仍然是以是否侵犯个人隐私作为处理个人信息的标准。然而，个人信息权是独立于隐私权之外、内涵更加丰富的概念。另外，现代信息技术为数据处理提供了更多可能，即使裁判文书仅披露少量个人信息，尚不足以达到严重侵犯隐私的程度，但通过相关信息技术的运用，仍然可能据此识别出特定个人。在公开裁判文书的过程中，应当对此予以考虑。

---

**Abstract:** It is of great significance to reasonably determine the boundary of criminal liability for the processing of publicly disclosed personal information. The theory of second authorization fails to accurately understand the provision of judicial interpretation, resulting in a too broad range of penalty. It also could not explain why and how the initial obtaining and the re-offering of publicly disclosed personal information should be treated differently. Although the theory of conformity to purpose seems more logical, it is difficult to judge and grasp the conformity to purpose of disclosure of personal information in practice. In situations where the information has already been objectively disclosed, imposing requirement and obligation of conformity to purpose on the processor of the information will compress the space for information freedom. The standard of general accessibility adopted by the German Federal Data Protection Act balances the protection of personal information with the guarantee of information freedom. This standard is relatively objective, clear and easy to be identified. In the position of protecting the right to personal information and based on the categorized analysis of publicly disclosed personal information, the degree of objective openness of information should be adopted as the criteria to uniformly determine the criminal liability for information processing. When examining the legality of the processing of publicly disclosed personal information, we should not only focus on the behavior of downstream information processing, but also reflect on the rationality of the criteria on the upstream disclosure of information.

**Key Words:** publicly disclosed personal information, second authorization, conformity to purpose, generally accessible, degree of objective openness

---

[66] 参见刘练军：《裁判文书公开时诉讼参与人信息的处理》，《法治现代化研究》2017年第6期，第152页；党德强、靳琳琳：《网络公开裁判文书与个人信息保护研究》，《山东行政学院学报》2020年第5期，第63页。

[67] 参见前引〔65〕，韩朝炜等文，第96页。

[68] 处理个人信息的比例性原则已经得到我国法律的确认，例如个人信息保护法第6条、第34条，民法典第1035条第1款。