

# 《民法典》视域下侵犯公民个人信息罪的司法适用

喻海松

**【摘要】**作为重要的前置法,《民法典》关于个人信息保护的规定,对侵犯公民个人信息罪的司法适用必将会产生重大影响。关于个人信息民法保护的立法思路,将对侵犯公民个人信息罪的司法适用,特别是政策把握产生重大影响。关于个人信息处理规则的设定,将直接影响侵犯公民个人信息罪前提要件“违反国家有关规定”的认定和其他构成要件的把握。关于个人信息的范围界定,特别是私密信息和非私密信息以及公开信息与非公开信息的划分,将直接影响侵犯公民个人信息罪的犯罪对象界定和其他构成要件的把握。

**【关键词】**《民法典》;侵犯公民个人信息罪;私密信息;公开信息;司法适用

**【作者简介】**喻海松(1980-),男,湖南新邵人,博士,最高人民法院研究室刑事处处长,研究方向为刑法、刑事诉讼法、网络与信息法、环境资源法(北京 100745)。

**【原文出处】**《北京航空航天大学学报》:社会科学版,2020.6.1~8

## 一、引言

法律是时代的产物。作为一部制定于21世纪的《民法典》,与法国《民法典》反映农业社会的要求、德国《民法典》反映工业社会的要求有所不同,中国《民法典》回应了当前信息经济和大时代的要求。最为突出的表现之一,就是基于互联网大数据时代保护个人信息的现实需要,《民法典》系统确立了个人信息保护制度:一方面,在第一编“总则”第五章“民事权利”规定“自然人的个人信息受法律保护”(第111条);另一方面,在第四编“人格权”第六章“隐私权与个人信息保护”用六个条文(第1034条至1039条)对个人信息保护作了详细规定。这就在法律层面真正系统地确立了个人信息保护制度并明确自然人对其个人信息享有人格权益,不仅对加强公民个人信息保护和促进信息产业发展具有重要意义,而且为正在制定之中的《个人信息保护法》《数据安全

法》奠定了坚实基础。

刑法是“最后的手段”,是典型的“二次法”和“保障法”,其适用通常要以前置法作为前提和基础。《民法典》是《刑法》的主要前置法之一,对其适用必然会产生重大影响。2009年2月《刑法修正案(七)》增设了《刑法》第253条之一,规定了出售、非法提供公民个人信息罪和非法获取公民个人信息罪;2015年8月《刑法修正案(九)》对《刑法》第253条之一作了修正,将罪名整合为侵犯公民个人信息罪。作为典型的法定犯,侵犯公民个人信息罪的适用无疑会受到《民法典》关于公民个人信息保护相关规定的影。特别是,侵犯公民个人信息罪的法条设置属于典型的空白罪状立法模式,无论是“违反国家有关规定”的认定,“公民个人信息”内涵和外延的把握,抑或侵犯公民个人信息罪行为方式的界定,均应当以包括《民法典》在内的前置法律法规为基础,以确保公民

个人信息保护实现法秩序的统一<sup>①</sup>。

基于此,文章拟以《民法典》关于公民个人信息保护的规定为基础,就其对侵犯公民个人信息罪的司法适用产生的影响加以论述。文章认为,相关影响可以概括为如下三个方面:第一,关于个人信息民法保护的立法思路,将对侵犯公民个人信息罪的司法适用、特别是政策把握产生重大影响;第二,关于个人信息处理规则的设定,将直接影响侵犯公民个人信息罪前提要件“违反国家有关规定”的认定和其他构成要件的把握;第三,关于个人信息的范围界定,特别是私密信息和非私密信息以及公开信息与非公开信息的划分,将直接影响侵犯公民个人信息罪的犯罪对象界定和其他构成要件的把握。

## 二、《民法典》关于个人信息的立法思路对刑法适用的影响

作为主要的前置法,《民法典》关于个人信息立法思路必然会对侵犯公民个人信息罪的司法适用产生影响。虽然此种影响可能不如后文将要提及的《民法典》相关具体规定的影响那么直接,但却是刑事司法者应当着力把握的。惟有如此,才能使得侵犯公民个人信息罪的司法适用与《民法典》关于个人信息保护的规定在旨趣上实现一致。

### (一)兼顾个人信息保护与促进信息自由流通

关于个人信息的立法,现代各国面临的首要问题均是如何平衡个人信息保护与促进信息自由流通之间的关系,中国亦不例外。一方面,当前个人信息滥用现象突出,保护自然人的个人信息不受侵犯是立法的重要任务;另一方面,在大数据和云计算时代,包括个人信息在内的数据,只有充分地流动、共享、交易,才能实现集聚与规模效应,最大程度地发挥价值。因此,在以互联网为代表的信息技术迅猛发展,巨量的个人信息数据日渐成为具有重大价值的生产要素的背景下,如何妥当处理好个人信息保护与信息自由流通之间的关系,也是《民法典》制定过程中着力寻求的平衡点。

关于自然人对其个人信息享有的究竟是民事权

利抑或仅仅是受保护的民事利益,民法理论界素有争议<sup>[1]</sup>。对于此前《民法总则》第111条规定的个人信息,就有学者主张“是个人信息权,而不是个人信息利益”<sup>[2]</sup>。在《民法典》编撰过程中,对于应否设置专门的个人信息权,也有不同看法。实际上,从世界各国的情况来看,法律都不会赋予自然人对其个人信息的排他支配权,“因为这样的授权会产生‘非经个人(也称为数据主体)同意,不得使用个人信息’的法则。在这样的法则下,许多人类社会活动无从开展”<sup>[3]</sup>。《民法典》最终未明确将个人信息规定为“个人信息权”,而是采用了“个人信息保护”的表述,并将自然人的个人信息权益归属于人格权益,就是认为“个人信息受保护的权利与其他人格权在考量因素上有所不同,个人信息的保护要适当平衡信息主体的利益和数据共享利用之间的关系”,旨在“既强调了对信息主体利益的保护,又可以避免不必要的误解,避免妨害数据的共享、利用以及大数据产业在我国的发展”<sup>[4]</sup>。特别是在具体制度设计上,《民法典》区分个人私密信息与非私密信息、公开的个人信息与非公开的个人信息,分别采用不同处理规则,并明确处理个人信息的免责情形,这些都体现了在有效保护个人信息的前提下兼顾促进信息自由流通和信息网络经济发展的现实需要。

就刑法适用而言,办理侵犯公民个人信息刑事案件,特别是对相关获取、提供公民个人信息行为定性时,要对标《民法典》的相关规定,坚决防止将符合《民法典》规定的行为认定为“违反国家有关规定”,甚至按照犯罪处理。更为重要的是,在刑事司法中也要贯彻平衡保护个人信息与促进信息自由流通的观念,对于一些处于模糊地带、法律规定不明确的案件,尽量秉持刑法的谦抑性,既要有力保护个人信息,也要防止动用刑法对信息自由流动的不利影响。

### (二)回归个人信息保护民法优先的应然状态

如前所述,侵犯公民个人信息罪属于典型的法定犯,理想的状态应当是先有前置法,后由作为“其

他部门法的保障法”的刑法加以规制。然而,受制于中国立法的现实情况,侵犯公民个人信息罪的前置法“供给不足”,甚至呈现出“刑法先行”的局面。早在2009年2月,《刑法修正案(七)》先于其他部门法明确了公民个人信息犯罪的界限,而后才有对网络公民个人信息保护作出集中规定的《网络安全法》自2017年6月1日起施行,但专门的《个人信息保护法》迄今尚未出台<sup>②</sup>。庆幸的是,这一趋势由于《民法典》关于个人保护的集中系统规定而得以扭转,使得个人信息保护回归“民法优先”的应然状况。特别是,《民法典》明确自然人对其个人信息的权益属于民事权益,扭转了在《民法典》之前由于个人信息保护多由行政管理法律法规加以规定,而认为自然人对其个人信息享有的是公法上权利的主张。作为调整平等民事主体之间社会关系的基本法,《民法典》的相关规定为其他法律关于个人信息保护的规定奠定了坚实基础。无论是基于行政法律法规对个人信息的处理,还是刑法关于侵犯公民个人信息罪的适用,都应当以个人信息的民事权益保护为基础,回归到平等的民事主体之间的法律关系上来,这对于加强个人信息保护、切实维护个人信息权益具有重大意义。

就个人信息保护而言,通过刑法积极适用防止侵犯公民个人信息违法犯罪持续蔓延,是不得已而为之的举措,但并非上策。刑法只能治标,尚难治本。《民法典》关于个人信息保护的相关规定,使得个人信息的刑事保护有了坚实的前置法基础。而且,一段时期以来由于前置法律规定缺失导致侵犯公民个人信息罪的司法适用存在相当争议的状况也会得以缓解,如后文所述对涉私密信息概括告知同意收集行为的定性、涉公开个人信息案件的处理等。此外,可以预见,在《民法典》厘清基本争议问题之后,《个人信息保护法》《数据安全法》将会得以顺利推进,公民个人信息民事、行政、刑事的全方位保护体系将会得以构建,公民个人信息违法犯罪的系统治理将会进入新的阶段。

### 三、《民法典》关于个人信息处理的规则对刑法适用的影响

(一)《民法典》关于“个人信息的处理”的界定与侵犯公民个人信息罪的行为方式

《民法典》将与个人信息相关的行为统一界定为“处理”,第1035条第2款规定:“个人信息的处理包括个人信息的收集、存储、使用、加工、传输、提供、公开等。”与之不同,《刑法》第253条之一规定的侵犯公民个人信息罪,在客观方面表现为两类行为方式:一是提供,即《刑法》第253条之一第1款、第2款规定的“出售或者提供”公民个人信息。出售也是提供的一种方式,实际上是有偿提供,是提供的常见类型<sup>③</sup>。此外,《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》(法释[2017]10号,以下简称《侵犯公民个人信息罪解释》)第3条第1款将“通过信息网络或者其他途径发布公民个人信息的”方式亦解释为“提供”。二是获取,即《刑法》第253条之一第3款“窃取或者以其他方式非法获取公民个人信息”。《侵犯公民个人信息罪解释》第3条第1款将“购买、收受、交换等方式获取公民个人信息,或者在履行职责、提供服务过程中收集公民个人信息的”方式亦解释为“获取”。

基于上述分析可以认为,《民法典》规定的个人信息的“收集、存储、使用、加工、传输、提供、公开等”,与《刑法》规定的侵犯公民个人信息罪的行为方式大致对应情况如下:①“收集”对应《刑法》规定的“获取”;②“提供、公开”对应《刑法》规定的“提供”;③“存储、使用、加工、传输”无法与《刑法》规定的行为方式对应。第③类行为方式可以概括为使用公民个人信息。实际上,在《刑法修正案(九)(草案)》研拟和审议过程中,有关部门和专家学者即建议借鉴国外立法例,将非法使用公民个人信息的行为入罪。然而,上述建议最终未被《刑法修正案(九)》采纳<sup>④</sup>。根据罪刑法定原则的要求,由于《刑法》第253条之一只是将非法获取、提供公民个人信息的行为入罪,对于实践中业已出现的非法存储、使用、加工、传输大

量公民个人信息案件,则难以直接入罪。当然,如果根据在案证据,适当运用推定规则,证明涉案公民个人信息系非法获取或者用于非法提供的,则可以适用侵犯公民个人信息罪。

(二)《民法典》关于个人信息的处理规则与侵犯公民个人信息罪“违反国家有关规定”的认定

《民法典》采用了世界各国个人信息保护所普遍确立的告知同意规则,在第1035条第1款第1项规定除法律、行政法规另有规定的外,处理个人信息应当征得该自然人或者其监护人同意。从实践来看,信息主体同意的方式可以多种多样;如后所述,个人信息的类型不同、重要程度有异,在征得信息主体同意的方式和程度上也会有所差异。而且,根据第1038条第1款的规定,信息处理者对于经过加工无法识别特定个人且不能复原的个人信息,可以不经该自然人同意向他人提供。此外,根据第1035条第1款的规定,处理个人信息,还应当遵循合法、正当、必要原则,不得过度处理,并符合公开处理信息的规则,明示处理信息的目的、方式和范围,不违反法律、行政法规的规定和双方的约定。上述要求与《网络安全法》第41条、第42条的规定基本一致。

根据《刑法》第253条之一第1款、第2款的规定,“违反国家有关规定”提供公民个人信息的,可以构成侵犯公民个人信息罪。根据第3款的规定,“非法”获取公民个人信息的,可以构成侵犯公民个人信息罪。根据《侵犯公民个人信息罪解释》第4条的规定,此处“非法”的判断也应当还原为“违反国家有关规定”。故而,侵犯公民个人信息罪的前提要件实际上可以概括为“违反国家有关规定”。值得关注的是,《刑法修正案(九)》(草案一次审议稿)将提供个人信息入罪的前提要件设置为“未经公民本人同意”,即采用的是主观判断的标准;但是,从《刑法修正案(九)》(草案二次审议稿)开始,采取了客观判断标准,即“违反规定”;《刑法修正案(九)》延续了这一立场,调整为“违反国家有关规定”。如前所述,法律不应赋予自然人对其信息享有排他的权益,故在刑法修法过程

中将侵犯公民个人信息罪的前提要件由主观标准调整为客观标准,无疑是妥当的。

“违反国家有关规定”,是指违反了有关法律、行政法规、规章等国家层面涉及公民个人信息管理方面的规定<sup>71</sup>。《侵犯公民个人信息罪解释》第2条进一步明确“国家有关规定”包括法律、行政法规、部门规章在内。在《民法典》第1035条对个人信息处理明确了规则之后,关于侵犯公民个人信息罪“违反国家有关规定”的判断应当以上述规定为基础。需要注意的是,《民法典》关于处理个人信息应当遵循的原则和条件较多,重要程度存在差异。故而,对违反相关原则和条件处理个人信息行为的刑事定性,在刑事违法和社会危害程度方面也会存在差异,不宜一概而论:鉴于告知同意是个人信息保护的核心原则,对于违反告知同意规则和违反法律、行政法规的禁止规定和双方的约定获取、提供公民个人信息的,可以认定为符合侵犯公民个人信息罪的前提要件“违反国家有关规定”;但是,对于违反必要原则、公开处理信息的规则以及明示处理信息的目的、方式和范围获取、提供公民个人信息的,是否符合侵犯公民个人信息罪的“违反国家有关规定”,宜综合考量社会危害性程度,根据案件具体情况作出妥当处理。

(三)《民法典》关于信息主体权益的规定与侵犯公民个人信息罪的适用

《民法典》规定自然人对自己的个人信息享有一系列权益。其中,除了前述第1035条规定的知情同意权外,第1037条规定了查阅复制权和更正删除权。需要注意的是,与《网络安全法》第43条的规定相同,自然人对个人信息的删除权不同于欧盟的个人信息“被遗忘权”,只限于“自然人发现信息处理者违反法律、行政法规的规定或者双方的约定处理其个人信息的”情形。

从刑法的适用来看,对于自然人要求查阅或者复制其个人信息,或者要求更正错误的信息,以及删除相关信息,而信息处理者未予履行的行为,似乎难以直接适用侵犯公民个人信息罪。究其原因,就在

于侵犯公民个人信息罪的客观行为方式表现为非法提供或者获取。当然,对于上述情形,如果根据相关证据证明存在非法获取或者提供公民信息的,则可以适用侵犯公民个人信息罪。

#### 四、《民法典》区分私密信息与非私密信息对刑法适用的影响

##### (一)《民法典》关于私密信息与非私密信息的界分

从域外个人信息法律保护模式来看,美国主要采取隐私权保护模式,以隐私权为基础,通过大量判例逐步构建起了一套保护制度。而欧盟关于数据信息的保护,则是从法律上将数据信息视为人格权的延伸<sup>[8]</sup>。中国《民法典》借鉴了后一种立法模式,将自然人对其个人信息的权益归入人格权的范畴,将个人信息保护与隐私权并列规定。个人信息与个人隐私之间虽有交叉但亦有区别,交叉部分就在于隐私中的个人私密信息属于个人信息的范畴。中国法律关于个人信息与个人私密信息之间关系的规定,历经了从明确规定到隐性规定再回归明确规定的阶段,可谓“否定之否定”的路径。

##### 1. 明确规定个人信息包括个人私密信息

2012年12月《全国人民代表大会常务委员会关于加强网络信息保护的决定》第1条第1款规定:“国家保护能够识别公民个人身份和涉及公民个人隐私的电子信息。”可见,这一界定将个人信息界定为“身份信息+隐私信息”,即将隐私信息明确为个人信息的范畴。受其影响,2013年4月《最高人民法院、最高人民检察院、公安部关于依法惩处侵害公民个人信息犯罪活动的通知》(公通字[2013]12号)第2条明确规定:“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. 未明确个人信息包括个人私密信息,但可以推断出这一结论

2016年11月《网络安全法》第76条规定:“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。”可见,《网络安全法》关于“个人信息”的界定,并没有明确涉及私密信息,而仅指向“身份识别信息”。显然,此处规定的“身份识别信息”应作广义理解,自然应当包括私密信息和其他活动情况信息在内。基于此,《侵犯公民个人信息罪解释》第1条规定:“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。”

##### 3. 回归明确规定个人信息包括私密信息的立法模式

《民法典》第1032条第2款对隐私作了明确界定,规定:“隐私是自然人的私人生活安宁和不愿为他人知晓的私密空间、私密活动、私密信息。”《民法典》第1034条第2款对《网络安全法》第76条关于个人信息的界定作了适度调整,将指向的“识别自然人个人身份的各种信息”调整为“识别特定自然人的各种信息”,即删除“个人身份”的表述,以防止将个人信息误解为狭义的身份识别信息。在此基础上,《民法典》第1034条第3款明确个人信息包括私密信息,规定:“个人信息中的私密信息,适用有关隐私权的规定;没有规定的,适用有关个人信息保护的规定。”这就标志着中国法律关于个人信息的界定,又重回将个人私密信息明确规定个人信息的立法模式,正式在基本法律中确立了私密信息与非私密信息的界分。

##### (二)《民法典》区分私密信息与非私密信息对刑法适用的影响

无论前置法采用何种立法模式,司法实务均认为公民个人信息包括个人私密信息在内,对于非法获取、提供个人私密信息的行为在刑法适用上完全

可以构成侵犯公民个人信息罪。从这个角度而言,可以认为,《民法典》区分私密信息与非私密信息的界分,对侵犯公民个人信息罪的适用不会产生大的影响。但是,立足于细微层面而言,侵犯个人私密信息刑事案件的处理,与其他侵犯公民个人信息刑事案件相比,还是会有较大差异。

具体而言,对个人私密信息优先适用隐私权的有关规定。根据《民法典》第1034条第2款的规定,对于个人私密信息优先适用《民法典》关于隐私权的规定,只有在相关规定欠缺的情况下,才适用关于个人信息保护的规定。根据《民法典》第1033条第5项的规定,处理他人的私密信息,除法律另有规定的情形外,须经权利人明确同意。可见,对于个人私密信息,《民法典》在保护力度上明显强于个人非私密信息,对后者的处理采用的是告知同意规则,即征得自然人或其监护人同意。“‘明确同意’与‘同意’的涵义是不同的。一方面,明确同意意味着自然人在被告知私密信息将被处理的前提下而作出清晰、明确的允许处理的意思表示。另一方面,明确的同意应当是针对该私密信息被处理而单独作出的同意的意思表示”<sup>[9]</sup>。司法实践中处理涉个人私密信息的刑事案件,在认定是否“违反国家有关规定”时,在除法律另有规定的情况下应当采用权利人“明确同意”的判断规则。例如,对于App将告知同意的内容置于冗长的隐私政策之中,导致用户实际上不会真正去了解隐私政策而选择同意,进而获取相关个人信息的行为,如何判断获取信息行为的性质素有争议。基于互联网时代获取个人信息的现实情况,要求逐项告知收集信息内容并征得同意似不可以,故对于个人非私密信息而言,上述行为难以认定为非法获取;但是,对于个人私密信息而言,由于《民法典》明确要求经权利人“明确同意”,采取上述方式收集个人私密信息的则可以认定为非法获取。

### 五、《民法典》区分公开的与非公开的个人信息对刑法适用的影响

一段时间以来,涉公开个人信息案件的处理是

侵犯公民个人信息罪司法适用中的最为棘手的问题之一。例如,行为人从商贸网站和政府部门公开的企业信息网上收集企业公开发布的信息(涉及自然人信息),将上述信息存入数据库,供他人付费查询使用。又如,行为人将房屋租赁网站上已经公开的房屋信息收集,将上述信息用于营利活动。上述案件的处理即存在较大争议,各方意见不一,处理结果有异。笔者主张,在《民法典》明确区分公开的个人信息和非公开的个人信息,并为二者设置了不同的处理规则的背景下,应当对标上述规定,妥当处理相关刑事案件。

(一)《民法典》关于公开的个人信息界定对刑法适用的影响

《民法典》第1036条规定:“处理个人信息,有下列情形之一的,行为人不承担民事责任:……(二)合理处理该自然人自行公开的或者其他已经合法公开的信息,但是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……”据此,个人信息分为公开的个人信息和非公开的个人信息。需要注意的是,公开的个人信息限于“合法公开的信息”,既包括自然人自行公开的信息,也包括其他途径合法公开的信息。前者如律师将自己的联系电话、通讯邮箱、办公地址等信息通过互联网或者其他途径公开,后者如依据行政行为、司法行为或者其他缘由而公开。不论以何种形式进行公开,公开的个人信息都限于通过合法途径公开的个人信息,而不包括非法公开的个人信息。

在办理涉公民个人公开信息的案件时,要注意查明相关公开的个人信息是否属于合法公开的信息,从而准确判断后续获取或者提供行为定性应当适用的规则。例如,对某住宿网站采取黑客攻击手段,非法获取住宿记录并通过互联网公开的,相关信息虽然客观上处于公开状态,但由于公开手段系非法手段,不属于前述“公开的个人信息”,对于行为人获取或者提供相关信息的行为定性,除后文所述认识错误的情况外,仍然应当适用非公开的个人信息

的判断规则。

侵犯公民个人信息罪系故意犯罪,以行为人具有主观明知为前提。刑法适用中需要注意的是,对于相关个人信息是否合法公开,既要从客观上进行查证,也要查明行为人的主观认识。一般而言,对于客观上公开的个人信息是否系合法公开,行为人未必能够认识到,对此要防止客观归罪。对于非法公开的个人信息,无法证明行为人主观上认识到,且一般人也难以认定到的,则应当按照有利于被告人的处理规则,可以适用公开个人信息的处理规则认定行为性质。

(二)《民法典》关于公开的个人信息处理规则的规定对刑法适用的影响

《民法典》区分非公开的个人信息与公开的个人信息,就在于两类个人信息的处理规则有异:对于非公开的个人信息,根据《民法典》第1035条第1款的规定,除法律、行政法规另有规定的外,处理相关信息需要征得该自然人或者其监护人同意;对于公开的个人信息,根据《民法典》第1036条第2项的规定,除自然人明确拒绝或者处理相关信息侵害其重大利益的外,合理处理相关信息不需要征得该自然人或者其监护人的同意。可见,《民法典》关于公开的个人信息保护强度要明显弱于非公开的个人信息。《民法典》的上述规定,为刑法适用中涉公开的个人信息案件定性的若干争议问题厘清了前置法规定。

在以往的刑事司法实践中,对于公开的个人信息,由于信息已经处于公开状况,获取无须征得同意,对此应无疑义;但是,在获取相关公开信息后进而提供的行为,是否需要取得“二次授权”(即在获取相关信息后,提供相关信息需要告知同意),则存在较大争议。可以说,《民法典》为这一争议问题作了明晰,即否定“二次授权”的规则。民法典第1038条第1款规定:“信息处理者……未经自然人同意,不得向他人非法提供其个人信息……”此处的“二次授权”,明显是针对非公开的个人信息而言。根据《民法典》第1036条第2项的规定,对公开的个人信息

合理处理可以推定自然人概括同意,即除了“该自然人明确拒绝或者处理该信息侵害其重大利益的”情形外,不需要通知和征得该自然人或者其监护人同意。据此,在处理相关刑事案件时,对于未通知并征得自然人同意而获取、提供公开的个人信息案件,只要行为人的获取、提供行为处于“合理”限度之内,除证明该自然人明确拒绝<sup>③</sup>或者相关获取、提供行为侵害了该自然人的重大利益的外,应当认为相关获取、提供的行为属于合法行为,不属于“违反国家有关规定”获取、提供公民个人信息的行为,更不应当认定为构成侵犯公民个人信息罪。

值得探讨的是,对于《民法典》第1036条第2项规定的“合理处理”的认定,应当采用相对宽泛的理解。原则上,只要法律、法规没有明确禁止的处理行为,均可以认定为“合理处理”,至少不能认定为犯罪。特别是,从保护信息自由流通的角度出发,要切实防止只要获取个人信息后进行营利活动或者超越信息初始公开使用场景的,即认为超越了合理处理界限的极端认识。例如,部分工商企业信息中包含有法定代表人姓名、联系电话等内容,属于公民个人信息的范畴。相关信息可以在“国家企业信用信息公示系统”中查询,已处于合法公开的状况。从初始的公开使用场景而言,确实限于在国家企业信用信息公示系统公开,方便民众查询以确认企业信息是否真实有效。以往刑事司法实践中,一些收集工商登记信息,未经自然人同意超越初始公开场景使用的情形,被认定构成侵犯公民个人信息罪。对此,笔者曾主张:“鉴于此类案件具有相当普遍性,未来的公民个人信息保护法和相关法律法规宜对公民个人公开信息的问题作出明确规定,以便利相关案件的处理。”<sup>④</sup>在《民法典》对公开的个人信息处理规则作出明确规定的情况下,对于上述案件,如果相关信息在公开时没有明确限定公开场景(即没有明确拒绝他人收集后在其他场景下使用),则对于收集并在未通知和征得该自然人同意情况下提供相关信息的行为,宜认为仍在“合理处理”的范畴之内。

总而言之,根据《民法典》关于界分公开个人信息和非公开个人信息的相关规定,要求刑法适用中妥当处理涉公开的个人信息的案件。一般而言,由于公开个人信息的案件侦办难度相对较小且涉案信息数量、违法所得等往往巨大,司法实践易以此类案件为打击重点。可以说,《民法典》的相关规定对于扭转这一趋势奠定了基础。在中国侵犯公民个人信息违法犯罪泛滥和公民个人信息保护水平整体不高的当下,对标《民法典》的相关规定,侵犯公民个人信息罪的司法适用应当以涉非公开个人信息的案件为重点,严厉惩治非法获取、提供非公开个人信息的案件,切实强化对公民个人信息的保护。

#### 注释:

①例如,《刑法》第253条之一未对“公民个人信息”的概念作出界定,这就决定了对其实质内涵和外延的把握必须受到前置法相关规定的影响。

②《个人信息保护法(草案)》已于2020年10月中旬提请十三届全国人民代表大会常务委员会第二十二次会议首次审议。

③对于《民法典》第1036条第2项规定的“明确拒绝”,宜理解为是事前的明确拒绝,即在该公开的个人信息被处理前明确拒绝。当然,由于处理多种行为方式、多个环节,只要在

特定的处理行为实施前明确拒绝即可。例如,在相关信息被收集后,可以明确拒绝后续的使用、加工、传输、提供等其他处理活动。

#### 参考文献:

[1]程啸.民法典编纂视野下的个人信息保护[J].社会科学文摘,2019(11):71—73.

[2]杨立新.个人信息:法益抑或民事权利——对《民法总则》第111条规定的“个人信息”之解读[J].法学论坛,2018(1):34—45.

[3]高富平.法律应如何保护个人信息[J].中国审判,2017(3):62—63.

[4]黄薇.中华人民共和国民法典释义(下)[M].北京:法律出版社,2020:1924.

[5]张明楷.刑法学(下)[M].北京:法律出版社,2016:922.

[6]喻海松.刑法的扩张——《刑法修正案(九)》及新近刑法立法解释司法适用解读[M].北京:人民法院出版社,2015:148.

[7]雷建斌.《中华人民共和国刑法修正案(九)》释解与适用[M].北京:人民法院出版社,2015:126.

[8]来小鹏.数据信息法律保护模式思考[J].中国审判,2017(3):60—61.

[9]程啸.我国《民法典》个人信息保护制度的创新与发展[J].财经法学,2020(4):32—53.

[10]喻海松.侵犯公民个人信息罪司法疑难之案解[J].人民司法(案例),2018(32):13—16.

## Judicial Application of Crime against the Citizens' Personal Information under the Perspective of Civil Code

Yu Haisong

**Abstract:** As an important up-level law, the provisions of the "Civil Code" on the protection of personal information will have a significant impact on the application of crime against the citizens' personal information. The legislative approach to the civil law on protecting personal information will have a momentous impact on the judicial application of the crime against the citizens' personal information, especially on the understanding of policies. The setting of rules for the processing of personal information will have a direct impact on the prerequisite of this crime, which is "violating the relevant provisions of the state". The scope of personal information, especially the division between private and non-private information, public and non-public information, will directly affect the definition of the object of crime and the constitutive elements about the crime against the citizens' personal information.

**Key words:** Civil Code; crime against the citizens' personal information; private information; public information; judicial application